TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

NO PUBBLICITÀ
SOLO INFORMAZIONE E ARTICOLI
2 €

n.172
HACKER JOURNAL
www.hackerjournal.it

CRACKING
LA DEBOLEZZA DEI SERIAL

SOFTWARE
3 VIRTUALIZZATORI A CONFRONTO

SOCIAL ENGINEERING
COME TI RUBO LA PASSWORD

STREAMING
FATTI LA TUA TV ONLINE



NOVITÀ DEBIAN 5

HACKING TEST
CHIAVE CRIPTATA DISTRUTTA MA NON BATTUTA

QUATTORD. ANNO 9 - N° 172 - 19 MARZO / 1 APRILE 2009 - € 2,00
WLF PUBLISHING

hack·er (hăk'∂r)
"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Il processo ai pirati

"Nei casi dubbi si decida per il giusto".
Karl Kraus

Si è concluso in questi giorni il dibattimento processuale che vede opposti i gestori di The Pirate Bay alla magistratura svedese, paese in cui risiedono i server del sito, e alle major musicali. L'accusa ha chiesto pene esemplari (risarcimento economico e un anno di galera per i "pirati"), la difesa ha invece chiesto la completa assoluzione per gli accusati.

Gli avvocati della difesa hanno sostenuto la legittimità della tecnologia che è alla base della Baia e particolarmente insistito su alcuni punti:

- *la decisione dell'accusa di non perseguire chi ha fisicamente commesso l'illecito, ovvero gli utenti, fa sì che l'intero processo sia basato sulla presunta complicità di un crimine in cui non è stato identificato un colpevole.*

- *Il fatto di conoscere qualcuno non significa necessariamente che si sia corresponsabili dei reati commessi da queste persone.*

Di fatto i gestori della Baia sono stati accusati di qualcosa che non è neppure stato stabilito sia o meno un crimine realmente avvenuto. Ricordo che sul sito non c'è mai stata l'effettiva messa a disposizione dei materiali coperti da diritto d'autore. L'accusa non ha saputo dimostrare l'illegalità dell'operato di The pirate Bay, ma il vero limite è che non ha saputo neppure capire fino in fondo come funzioni il protocollo BitTorrent.

Insomma, The Pirate Bay è legale oppure no?

Confuso? Comprensibile. Questo piccolo approfondimento tecnico-legale è solo per farti capire che la materia, che soffre indubbiamente di grandi vuoti legislativi, è comunque piuttosto complessa e non è certo risolvibile con poche battute o con processi. Non sono i processi a dover stabilire regole e leggi, ma il legislatore. La proprietà intellettuale è un bene che va tutelato, sia all'interno dei propri confini, sia rispetto all'uso applicato alle nuove tecnologie. Le leggi in materia dei singoli stati sono ancora troppo spesso "analogiche" e con principi applicabili ai tempi del vinile.

La sentenza è annunciata per il 17 aprile.

The Guilty

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa!
Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.172
19 marzo / 1 aprile 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Le losche magagne di Facebook

Le mezze misure sono diventate come le mezze stagioni: non ci sono più. Questo vale per Facebook: o lo si ama, o lo si odia, difficile trovare qualcuno ancora indeciso. Quello che è certo è che il boom di iscritti degli ultimi tempi, per quello che riguarda l'Italia, non è leggenda: è reale e documentato. Ma proprio questo boom di iscrizioni ha portato all'attenzione di tutti quelle che sono le pecche del sito per il social networking. Per prima cosa, è da tenere ben presente che una tecnologia non è maligna in sé, ma per l'uso che se ne fa. È stato accertato (ne abbiamo parlato in due occasioni) che si può sfruttare la piattaforma Facebook per scrivere applicazioni maligne, i cui risultati sono sì in questo caso incerti ma comunque è fattibile.

Ci tocca quindi fare attenzione ai moduli che andiamo a integrare nel nostro profilo: è notizia di questi giorni che altre due applicazioni inducano a scaricare e a installare software che si è rivelato essere un malware. Non solo: come vero e proprio specchio della società reale, Facebook presenta varie sfaccettature, tanto è variegata l'umanità che lo adotta come mezzo di comunicazione. Troviamo quindi gruppi che esprimono l'apprezzamento per questo o quell'artista, ma anche gruppi che inneggiano allo stupro di gruppo o che parteggiano per malavitosi e personaggi sinistri della nostra attualità.



Il Governo, in Italia, vorrebbe oscurare questi gruppi, ma sarebbe come tentare di imbavagliare Internet stessa: una cosa impossibile. C'è anche chi fa leva sul discorso privacy: Facebook è un ricettacolo di dati personali sensibili, e la maggior parte dei sei milioni e mezzo di italiani che lo usano non si rendono conto che i propri dati siano così a disposizione di tutti, basta una semplice ricerca su Google e si trovano i profili di tutti.

E, come ciliegina sulla torta, Facebook ha recentemente modificato le condizioni d'uso, per cui i contenuti che abbiamo nel tempo pubblicato sul sito diventano praticamente di proprietà della compagnia, che può usarli a proprio piacimento e in qualunque momento. Già era difficile prima scomparire da Facebook, ora appare quasi impossibile, con somma gioia del Garante della privacy. Per nostra fortuna, il grido di protesta di Garanti e di utenti è stato ascoltato da Mark Zuckerberg, il patron di Facebook, che ha ripristinato le condizioni precedenti e promesso che la prossima stesura delle stesse avverrà col contributo fondamentale degli utenti stessi.

UN ALTRO VERME PER SYMBIAN

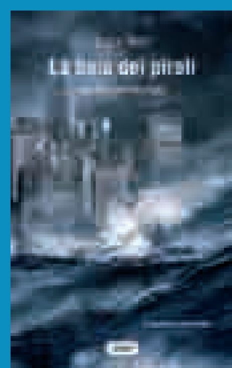
Premesso: per prendere un virus su cellulare bisogna essere proprio incoscienti. Fortinet, azienda specializza nel monitoraggio dei virus e spyware che minacciano il Web, ha segnalato una nuova grana per i possessori di smartphone Symbian s60 3°edizione che porta il nome di SexView. Se installato è in grado di prendere il controllo della rubrica, inviarsi a tutti i contatti sfruttando la rete GSM o la connessione Internet facendo crollare il credito sulla Sim. Il suo obiettivo principale è però quello di "fregare" alcuni dati sensibili del telefonino come il codice EMEI, il PIN, o le password memorizzate nel telefono, inviandole direttamente ai suoi creatori. Se siete così stolti da avviare sul vostro telefono un file che si chiama SexView... beh, ve lo siete cercati.



ULTIMISSIMA: I PIRATI CALANO SU ROMA

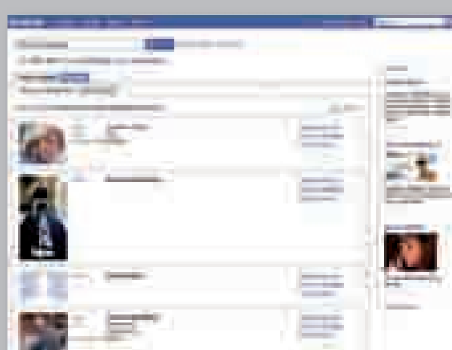
www.No-Copyright.net

Proprio al momento di andare in stampa abbiamo appreso che il giornalista Luca Neri, autore del libro "La baia dei pirati, Assalto al copyright" (2009, Edizioni Cooper), ha sfidato tutte le comunità italiane attive sul peer-2-peer, la critica alla proprietà intelletuale e la lotta per la libertà delle reti: *"Perché dobbiamo tacere quando i media ci dicono che la pirateria è un grave problema? La propaganda delle multinazionali dell'audiovisivo sostiene che chi scarica opere protette dal copyright è un ladro. Il governo sta studiando proprio in queste settimane nuove norme repressive. Eppure Cisco dice che due terzi di tutto il traffico Internet a livello mondiale sono generati dal p2p. Il downloading è un fenomeno che coinvolge milioni di persone anche in Italia. Non sarebbe l'ora di rovesciare i termini della questione? Di rivendicare a testa alta che i pirati non sono affatto i cattivi? Che sono invece i paladini della libertà digitale, della condivisione del sapere e della cultura? Che rappresentano il futuro?"*. La provocazione di Luca è stata ripresa con entusiasmo da associazioni come Scambio Etico/TNT Village e Partito Pirata. Ha suscitato un forte interesse fra molti membri di Frontiere Digitali e del Linux Club Italia. Siamo quindi in grado di anticiparvi che i pirati stanno complottando per organizzare un grande evento pubblico, "**La festa dei pirati**", sabato 28 marzo a Roma, che faccia da contro altare alle tesi oscurantiste della Commissione antipirateria del governo. Per saperne di più: http://www.no-copyright.net.



PRIVACY SU FACEBOOK... TENTATIVO FALLITO!

Facebook è di gran lunga la più importante comunità virtuale del pianeta con i suoi oltre 150 milioni di utenti. Un "bottino" troppo ghiotto per le aziende a caccia di dati personali e contenuti da recuperare senza chiedere nulla a nessuno. Facebook ha tentato di agevolare questa pratica ai limiti dell'illegalità inserendo una piccola clausola nel nuovo contratto delle condizioni d'uso che le avrebbe garantito di acquisire la proprietà intellettuale di tutti i contenuti postati sulle pagine del suo portale. Per capirsi, qualunque foto, video, canzone, poesia, o scritto di qualsiasi tipo inserito nella vostra pagina sarebbe diventato di proprietà di Facebook... diciamo sarebbe, perché molti utenti si sono accorti di questo "leggero" cambiamento del contratto e hanno denunciato Mark Zuckerberg, proprietario di Facebook per violazione del copyright. Poche ore dopo la clausola "criminale" è stata ritirata. Occhi aperti! Sempre.





HOT NEWS

LA NORVEGIA DIFENDE IL P2P

The Pirate Bay

La Norvegia è il nuovo paradiso del P2P. Mentre imperversa in tutta Europa la causa tra le case discografiche e il popolare portale Pirate Bay, il Partito Socialista Norvegese, nella persona di Bård Vegar Solhjell, Ministro dell'Educazione e della Cultura, prende una posizione totalmente opposta a quella delle major. Secondo Solhjell infatti il P2P non ucciderà il mercato musicale esattamente come non lo fecero 30 anni fa le cassette registrabili o le videocassette. La Norvegia inoltre sta pensando addirittura di legalizzare lo scambio di musica via P2P magari attraverso degli abbonamenti che forniscano agli utenti la possibilità di scaricare musica liberamente. Non c'è che dire... i Paesi nordici sono sempre 10 anni avanti a tutti.

BARBARESCHI CONTRO LA PIRATERIA



Luca Barbareschi, il popolare personaggio televisivo e deputato del PDL, ha presentato in parlamento una proposta di legge per fronteggiare il problema della pirateria digitale. La proposta, che ricalca esattamente quella "scritta" dalla SIAE poche settimane fa, porterebbe un severo giro di vite al traffico dei dati sul web, coinvolgendo utenti, provider e forze dell'ordine. La pirateria, dice Barbareschi, deve essere "improcrastinabilmente bloccata" e a nulla servirebbe il neonato comitato creato dal governo per ragionare su questo delicato problema. Ci piace questa opinione "distaccata" del proprietario di una casa cinematografica e di una televisiva... e per i pirati, Barbareschi? La ghigliottina va bene, o si più fare di più?

IT'S A KIND OF MAGIC

Si chiamerà Magic e sarà distribuito a partire dal mese di marzo da Vodafone Italia. Si tratta del nuovo smartphone dotato di sistema operativo Android, sviluppato da Google. Magic, già noto con il nome in codice G2, è un cellulare avanzato con interfaccia touch, wi-fi e HSDPA che dovrebbe essere esente dai difetti che hanno decretato l'insuccesso del suo predecessore G1.



Tra questi le dimensioni e il peso più contenuti grazie all'eliminazione dell'ingombrante tastiera fisica sostituita da una comoda tastiera virtuale sullo stile di quella di iPhone. Per il resto le novità sono poche ma il G2 potrà vantare una quantità maggiore di programmi nello store di Google rispetto al G1 e all'introduzione della funzione street view nel sistema di mappe. Il prezzo non è stato ancora comunicato ma dovrebbe aggirarsi sui 400 euro.

Bullismo su XBOX Live



È sicuramente la notizia del mese. Il portale di giochi Xbox Live! accessibile dalla console di Microsoft è diventato il posto meno sicuro su cui giocare. Alcuni hacker infatti, probabilmente delusi dalle loro scarse performance ai titoli più famosi, hanno deciso di "giocare sporco" danneggiando, fino alla cancellazione dell'account, i player più bravi. Il sistema studiato dai pirati è molto comune sui PC, ma si tratta di una vera novità per le console: in pratica, ogni volta che giochiamo, comunichiamo al nostro avversario una serie di dati come ad esempio l'indirizzo IP della macchina. A questo punto è un attimo, per chi se ne intende, inviare un programmino che permetta di prendere il controllo, da remoto, dell'Xbox360 del suo avversario e utilizzare la sua gamertag come più gli aggrada: da qui, governare interi server è stato un gioco da ragazzi. Con questo metodo alcuni hacker hanno potuto eliminare da Xbox Live moltissimi utenti regolarmente iscritti, creare account pirati e addirittura "dettare legge" in particolari giochi in cui, se si alza troppo la testa, si viene bannati senza pietà. Bullismo insomma. Microsoft sta lavorando per risolvere il problema... vedremo.

COME TI FREGO LA BIOMETRIA

Acclamato come il sistema di sicurezza più avanzato al mondo, il riconoscimento biometrico si sta rivelando giorno dopo giorno un enorme bluff pieno di falle. A scoprire un altro punto debole questa volta sono stati i ricercatori della Hanoi University of technology, che, ad una recente conferenza hanno dimostrato quanto sia semplice imbrogliare le videocamere biometriche presenti su alcuni, costosissimi, notebook di nuova generazione. Le webcam sono in grado di analizzare i tratti del viso di chi è seduto davanti al pc e di estrarne delle caratteristiche uniche che in seguito gli permetteranno di accedere a documenti e file. Peccato che i ricercatori abbiamo dimostrato che basta una semplice immagine a colori, neanche troppo definita, della faccia del proprietario del computer per accedere ugualmente al suo PC. La videocamera infatti non è in grado di distinguere le persone "vere" dalle immagini: basta aver postato una propria foto sul Web oppure su Facebook, e... biometria addio!



IL BLACKBERRY DI OBAMA? CRACCABILISSIMO

Quando Barack Obama è diventato Presidente degli Stati Uniti, ha manifestato il desiderio di poter continuare ad utilizzare il suo Blackberry per comunicare con il suo staff e i suoi familiari. Infatti il regolamento della Casa Bianca prevede, per ragioni di sicurezza, che il presidente utilizzi altri strumenti di comunicazione per proteggere i segreti di Stato. Tuttavia con uno sforzo enorme gli esperti informatici di Washington hanno modificato il balckberry in modo che sia impenetrabile agli attacchi informatici, per la gioia di Obama. Tutto questo però, potrebbe non bastare. A dirlo è nientepopodimeno che Kevin Mitnick, il re degli hacker che, dopo qualche anno di prigione ha deciso di passare dalla parte dei "buoni". Secondo Mitnick, attaccando i computer,meno protetti, dei familiari o dei collaborato di Obama, degli hacker esperti potrebbero facilmente risalire all'indirizzo mail del Presidente e sviluppare qualche tipo di attacco per rubare tutti i dati contenuti nel blackberry. E se lo dice lui, c'è da credergli!



VIDEOGIOCHI VIOLENTI A GOGO... MA SOLO IN CALIFORNIA

La Corte federale della California ha giudicato inammissibile l'appello presentato dal Governo dello stato per rispolverare un vecchio decreto sulla classificazione dei giochi violenti. Il decreto prevedeva una nuova ridefinizione dei bollini di segnalazione che avrebbero dovuto segnalare "chiaramente" sulla scatola i giochi non adatti ai minori. A questo, e probabilmente è la cosa che più avrebbe danneggiato i rivenditori, si sarebbero aggiunte multe fino a 1000 dollari per i negozianti scoperti a vendere giochi proibiti ai minori. Le motivazioni della Corte sono state semplici: " perché allora non vietare anche giochi che inneggiano a comportamenti poco sani come mangiare cibi poco salutari, o usare delle buste di plastica". Insomma, vale il principio universale del buon senso... il compito di educare i ragazzi, è dei genitori, non dei governi di nessuna parte del mondo.



HOT NEWS

VISTA CAPABLE: HA VINTO MICROSOFT

Qualche settimana fa vi abbiamo parlato della causa intentata da alcuni utenti contro Microsoft, per il logo "Vista Capable" appiccicato su moltissimi computer alla fine del 2006. Le associazioni di consumatori consideravano truffaldino questo adesivo in quanto, molti PC, acquistati perché pronti per il nuovo Windows Vista, erano in realtà in grado di far girare solo Windows Vista Home Basic, un sistema operativo privo di tutte le funzionalità avanzate (Aero in primis) del "vero" Windows Vista. A salvare Microsoft è stata l'impossibilità da parte dell'accusa di produrre prove tangibili che il logo avesse influenzato le scelte dei consumatori, portandoli ad acquistare i computer con la promessa di poter, in seguito, installare Windows Vista. Il giudiche Perkins, che ha chiuso ufficialmente l'indagine, ha comunque richiamato Microsoft per aver dato informazioni confuse sulla reale possibilità di utilizzare Windows Vista su PC più datati, ma questo non poteva "valere" una condanna. Il dubbio resta: un giudice prima accetta un ricorso, spuntano fuori documenti compromettenti per Microsoft, e improvvisamente il ricorso non è più ammissibile... ma negli USA pare che la corruzione non esista, per cui tutto bene, no?



GLI U2 SI "PERDONO" L'ALBUM

Il nuovo album degli U2 intitolato "No Lines on Horizon" è uscito da pochissimi giorni, eppure alcuni fortunati fans australiani, hanno avuto la possibilità di scaricare legalmente il CD completo già dalla metà di Febbraio. La "colpa" è dell'amministratore di sistema di un sito collegato alla Universal (etichetta che segue Bono Vox e compagni) che ha inavvertitamente reso visibile la pagina da cui era possibile scaricare i brani del nuovo album. I download sono stati svariate migliaia dal momento che i responsabili della casa discografica si sono resi conto dell'errore dopo circa una settimana. L'uscita dei nuovi album è sempre ricca di imprevisti per gli U2 che già avevano visto uscire in anteprima le tracce del vecchio CD a causa di uno "zelante" fan che era riuscito a registrare 4 brani dell'album direttamente dallo stereo di Bono appostandosi sotto casa sua.



LA SIAE ELIMINA I BOLLINI

Le opere di ingegno (CD, DVD, libri, riviste e altro ancora) non necessitano del bollino SIAE per essere ritenute in regola. Questa epocale sentenza arriva dalla Corte di Giustizia Europea che ha accolto la tesi per cui "non esiste alcun obbligo,in carico al richiedente di licenze opera per opera, o sulla base di contratto generale, di provvedere all'acquisto di contrassegni in occasione dell'acquisizione delle licenze presso le sedi SIAE". Questo vuol dire anche chi i produttori discografici non dovranno pagare soldi in più per inserire su ogni singolo CD il bollino SIAE. Che poi questo si ripercuota su una diminuzione dei prezzi della musica e dei video in DVD.. bhe, questo è tutto un altro discorso!



SCARICARE LIBRI DA GOOGLE

Google Books è il servizio di Google che permette di sfruttare il motore di ricerca per consultare rapidamente testi, manuali, o opere di letteratura alla ricerca di un'informazione o una citazione. Da oggi però è addirittura possibile scaricare interi libri in formato PDF, grazie all'accordo di licenza stipulato con la società americana autori ed editori. Per il momento il download è consentito solo per i libri su cui è decaduto il diritto d'autore, cosa che include però tutti i classici della letteratura mondiale. L'accordo tra Google e l'associazione degli editori, porterà presto alla creazione comune di numerose biblioteche virtuali, consultabili gratuitamente da tutti gli utenti della rete.

GMAIL CRASH IN EUROPA

Cosa succede se un dei principali servizi di posta elettronica del mondo si ferma per mezza giornata? Magari agli utenti comuni, poco o niente, ma per le aziende, enti e organizzazioni che si affidano alla webmail di Google quotidianamente rappresenta un danno consistente. Qualche giorno fa, l'incubo si è avverato: uno dei principali server di Google è stato chiuso per manutenzione rendendo inaccessibile la posta elettronica di milioni di utenti in tutta Europa. Di solito in questi casi, il server effettua uno "switch" automatico su un altro computer per garantire la continuità del servizio. Purtroppo questo non è avvenuto e Google è stata costretta a scusarsi con i suoi utenti per lo spiacevolissimo inconveniente. Ahi ahi ahi Google, non ci siamo proprio.



Di tutte le tecniche di hacking, quella del social engineering ha dato da sempre i migliori risultati

DAMMI LA PASSWORD

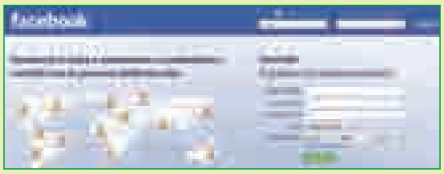
L'ingegneria sociale è da sempre una delle più pericolose e affascinanti tecniche di cracking disponibile. Non consiste nell'analizzare il software o l'hardware ma nel concentrarsi sul punto più debole dell'interazione uomo macchina: l'uomo. Il metodo di attacco segue sempre uno schema comune: acquisizione di informazioni, creazione di una identità fittizia, approccio alla vittima, infiltrazione e violazione dei sistemi. Per essere un bravo social engineer servono soprattutto faccia tosta, nervi saldi e capacità di mentire. Quello che segue è solo un racconto tra i tanti di un possibile attacco; inutile dire che le tecniche usate non sono sempre legali.

:: Ricerca

Individuato il bersaglio in un'azienda, e sapendo che qualsiasi tentativo di bucare le difese della società è destinato a fallire o a complicarsi enormemente visto che sono state già raccolte tutte le informazioni tecniche necessarie, escluse le password. Si passa alla prima fase, chiamata footprinting, che consiste nel raccogliere informazioni su chi, nella società vittima, può rappresentare un punto debole. In questo caso viene scelto il direttore del personale, una figura con abbastanza potere in azienda da essere significativo ai fini dell'attacco. Dopo qualche indagine sul Web si scopre che ha un profilo su Facebook da cui si ricava una lista di amici. Indagato sui suoi amici e si scopre che molti partecipano a gare di nuoto. Con un appostamento davanti alla società scopriamo che il soggetto si reca quasi tutte le sere in una piscina, a poca strada dall'ufficio, che è single, adora il sushi e tende a far tardi la sera. A questo punto ci sono tutte le chiavi per entrare in gioco.

:: Fondiamo una società

Usando un servizio di stampa online, per qualche euro si fanno stampare i biglietti da visita di una fantomatica società di consulenza software. Usando una mail online, si creano 5 blog su alcune delle piattaforme disponibili: uno con i colori dei biglietti da visita e gli altri con grafica varia. Si popola il tutto facendo sembrare i 4 blog minori come tenuti da singoli e società, anch'esse rigorosamente inventate, e usando il blog della società per pubblicizzare una serie di servizi di consulenza. Vengono collegati i blog minori a quello della società decantando il risparmio economico derivato dalla consulenza fatta.



Facebook, come tutti i social network, è una fonte di informazioni prodigiosa. Integrandolo con banali ricerche di Google si ottengono dati preziosi su chiunque o quasi.

Si preparano quindi alcune copie della brochure della nostra falsa società e ricorriamo a un servizio di segretarie virtuali per ottenere un indirizzo valido e un numero di telefono. Per finire si passa alla dotazione tecnica necessaria all'operazione: un portatile di nuova generazione dotato di scheda UMTS, VMWare, Hamachi e qualche tool di analisi. Lo scopo sarà quello di collegare il portatile alla LAN aziendale e permettere a un complice esterno di agire in background su una macchina virtuale per fare i suoi comodi.

:: A pesca

È tutto pronto e non resta che gettare l'amo, ad esempio la classica ragazza carina che inizia a frequentare la piscina alla stessa ora dell' obbiettivo. L'esca viene abbordata all'uscita della piscina dal nostro galante direttore del personale che le offre un caffè, seguito da una cena in cui la ragazza dice di lavorare per la fantomatica società, di essere una



Uno o più blog che diano l'idea di essere sul presenti sul mercato da tempo possono offrire una grande credibilità.

commerciale, e con nonchalance gli lascia la brochure e biglietto da visita.

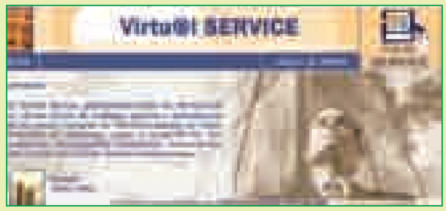
:: Presi!

La ragazza sta al gioco con il direttore per qualche giorno, in cui lascia intendere che ha diversi problemi di lavoro, è stressata e non può fare tardi la sera perché deve essere in ufficio prestissimo per dimostrare che sa fare il suo lavoro al suo capo a cui deve presentare un grosso cliente. Tempo altri due giorni e ariva un appuntamento col direttore generale della società vittima. Si presentano in tre: l'esca, ovviamente, e due tecnici. La trattativa va avanti illustrando le inesistenti qualità della finta struttura e, finalmente, uno dei tecnici dà un assaggio delle capacità di analisi in possesso facendo la domanda fatidica: "Se mi dà la sua password, le mostro come è possibile ottimizzare la gestione del flusso dei dati all'interno dell'azienda". Non vuol dire nulla ma il direttore ci casca in pieno e spiffera tutte le informazioni necessarie a collegare il portatile alla rete aziendale. Per incantare il direttore,



I tradizionali biglietti da visita sono indispensabili per costruirsi una falsa identità nel campo degli affari. A questi è meglio unire una brochure.

nel frattempo, usano un semplice programma di ping grafico reperito sul Web e poche altre stupidaggini che fanno molto effetto come schemi di Visio e tabelle di Excel, il tutto condito da milioni di parole.



Una segretaria virtuale è indispensabile per dare l'idea di una vera società. Sono disponibili anche servizi esteri localizzati in lingua italiana dove vengono fatte poche domande. Basta pagare.

Sul portatile, in background, sta invece operando, da un Internet Point, il complice esterno. La password gli viene passata scrivendola nel blocco note con lui in osservazione tramite un banale server VNC.



Strumenti di controllo remoto come VNC o Hamachi permettono all'attaccante che opera da una postazione estrena di lavorare con calma e al sicuro.

:: Sgancio lento

A questo punto, a sole due ore dall'ingresso nella società, riceviamo la telefonata che ci dà l'OK per iniziare l'operazione di sganciamento. Salutiamo la vittima promettendo un preventivo entro la settimana seguente. L'esca esce lentamente di scena. Nel frattempo arriva il salatissimo preventivo dell'inesistente società che, ovviamente, viene cestinato e la finta società può sparire nel nulla: il risultato (con un investimento di 500 € circa) è stato raggiunto: accesso totale alla rete aziendale con tutto quanto (d'illegale) ne consegue.

LA FORZA DELL'ELEFANTE



Pesante, lento ma potentissimo. Visual Studio 2008 Express Edition: gratis da Microsoft!

Per imparare a programmare o, se già lo sappiamo fare, per scrivere per conto nostro programmi utili o divertenti, serve un buon ambiente di sviluppo, meglio se integrato con un'interfaccia utente facile da usare. Se poi abbiamo a disposizione anche un'ampia documentazione in linea e possiamo attingere all'esperienza di moltissimi altri programmatori partecipando a forum e attingendo ad altre risorse sul Web, tanto meglio. Visual Studio 2008 Express Edition offre tutto questo e anche di più, al prezzo forse di un po' troppe risorse del computer.

:: Perché usarlo

Innanzitutto perché è lo strumento di sviluppo con cui è stata scritta la maggior parte del software per Windows da parte del produttore stesso, ovvero Microsoft. Se vogliamo quindi che il nostro programma appaia esattamente come una di quelle applicazioni professionali e performanti che siamo abituati a vedere sul nostro PC, non c'è niente di meglio che scriverlo usando gli stessi strumenti. Inoltre, come già detto, Visual Studio può contare su documentazione e aiuti che altri sistemi di sviluppo possono solo sognare, quindi è facile imparare a programmare con esso. La Express Edition non differisce molto dalle versioni commerciali e professionali, costosissime e inaccessibili per gli hobbisti e per chi sta imparando; pertanto possiamo contare su un ottimo ambiente di sviluppo per i nostri esperimenti. In più è gratis e completo: non solo IDE e un compilatore, come nella maggior parte dei casi, ma anche compilatori e strumenti come server database e un'ampia base di template e modelli da riutilizzare.

:: Download e installazione

A questa procedura dobbiamo dedicare una buona mezza giornata, e avremo un ambiente di sviluppo organizzato al meglio per le nostre necessità. Il download in sé non dura molto: se scegliamo di scaricare la ISO dell'intero Visual Studio, poco oltre 800 MB di file, non impiegheremo molto tempo grazie all'alta velocità del server Microsoft (abbiamo ottenuto punte da 1,1 Mbps e il download è durato circa un quarto d'ora). Non potremo estrarre i file contenuti nell'immagine scaricata in quanto si tratta dell'immagine di un DVD con file system UDF: dovremo quindi masterizzarla o usare un drive virtuale come Daemon Tools per montarla nel sistema. L'avvio automatico permette di scegliere i componenti da installare. Consigliamo di farlo nell'ordine indicato dalla schermata, dall'alto verso il basso, e di tenere a portata di mano qualcosa da leggere e da sgranocchiare dato che il tempo necessario è molto.

Un dato di fatto è che Visual Studio è pesante di suo: è un sistema complesso e composto da numerosi componenti, quindi più RAM e più potenza di calcolo possono solo aiutare, soprattutto in fase di compilazione.

:: L'interfaccia

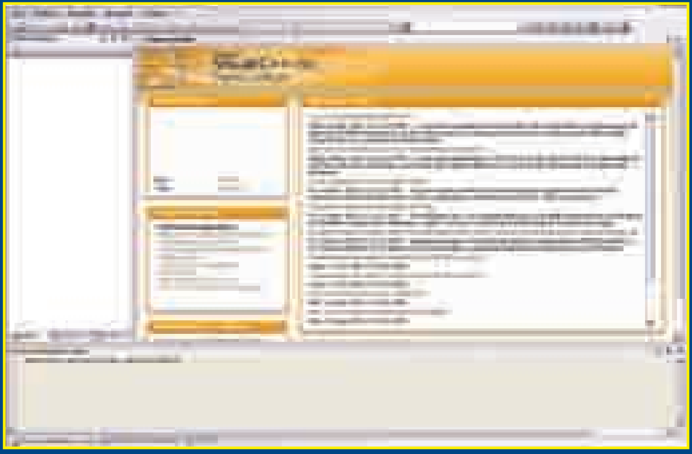
Anche se Visual Studio è composto da diversi compilatori e altri elementi, l'interfaccia di gestione è unica per tutto. È l'ambiente stesso che si occupa di richiamare di volta in volta il compilatore o lo strumento giusto secondo il caso. All'avvio, troviamo tre pannelli riposizionabili che contengono la struttura del progetto (nelle ultime versioni si chiamano soluzioni e non più progetti), un watch per le definizioni nel codice e un pannello centrale che visualizza il file su cui stiamo lavorando al momento. Non avendo ancora aperto alcuna soluzione, quest'ultimo pannello mostra i comandi principali e un elenco di news provenienti direttamente dall'area sviluppatori del sito Microsoft, utili per tenerci aggiornati: se non desideriamo più riceverle possiamo tranquillamente disabilitare tale funzione. Come d'uso ormai in ogni IDE che si rispetti, tutti i pannelli sono suddivisi in varie schede e sono ridimensionabili e riposizionabili secondo le nostre esigenze, quindi avremo sempre un ambiente di lavoro personalizzato e comodo da usare.

:: Cosa ci possiamo fare?

Visual Studio 2008 Express Edition comprende quattro compilatori utili per ogni tipo di programma: Visual C# (si legge "C sharp"), Visual Basic, Visual C++ e Visual Web Developer. Visual Basic è utile per imparare i fondamenti delle interfacce grafiche e della programmazione a oggetti ed è molto semplice da imparare. Visual C++ è lo strumento di programmazione per eccellenza, completamente a oggetti e usato per creare la maggior parte delle applicazioni per Windows, ma di difficile apprendimento. Visual C# si pone nel mezzo, unendo la versatilità del C++ con la facilità di programmazione del Basic, quindi può essere un utile "gradino di mezzo" nel passaggio da un linguaggio all'altro. Infine, Visual Web Developer è un ambiente espressamente dedicato a soluzioni per il Web, quindi a siti articolati e dinamici, soprattutto grazie all'appoggio diretto alle tecnologie di MS Sql Server (installato anch'esso in versione Express insieme agli altri strumenti). Dal semplice progettino fino all'applicazione complessa, giungendo anche eventualmente al sito Web per la sua distribuzione, questo è ciò che possiamo fare con questo prodotto. E, cosa molto interessante, non siamo vincolati da ragioni commerciali di sorta: se vogliamo vendere i nostri programmi creati con Visual Studio Express, possiamo farlo!



L'autorun del DVD di Visual Studio mostra l'elenco dei compilatori e degli strumenti che è impossibile installare.



Il "paginone centrale" di Visual Studio: nessuna coniglietta discinta, ma tante notizie dedicate agli sviluppatori da parte di Microsoft.

Naturalmente potremmo anche scegliere di installare solo uno dei compilatori e non tutti: in ogni caso la procedura di setup sa perfettamente di quali strumenti ha bisogno l'elemento scelto e li installa automaticamente. Scegliendo di installare tutto, un elemento alla volta, abbiamo impiegato una mezza giornata di lavoro. In realtà il computer usato per la prova non era molto performante, quindi non è escluso che in altre situazioni l'installazione risulti molto più veloce.



Tutti ne abbiamo una e tutti vorremmo riuscire a usarla senza che ci costasse come il pieno di una Ferrari

SCHIAVI DELLA STAMPANTE

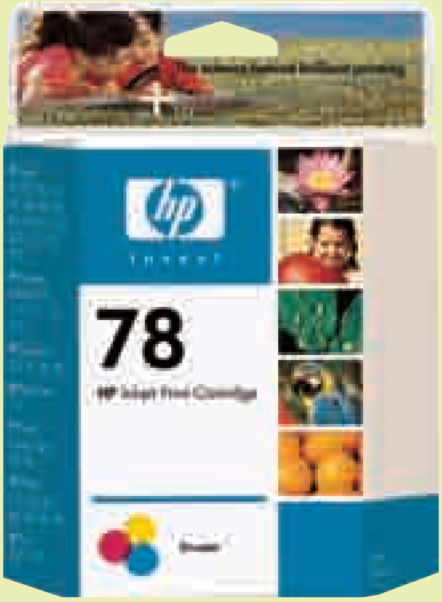
Quando torniamo a casa, dopo la scuola o il lavoro, troviamo spesso la cassetta della posta piena di volantini pubblicitari delle varie catene di ipermercati e centri commerciali della zona. Da buoni geeks, la prima cosa che andiamo a vedere è la sezione delle tecnologie di consumo, dai televisori all'informatica. E qui scopriamo che per veramente due soldi possiamo portare a casa una super stampante fotografica con tanto di display LCD a colori, sia a getto d'inchiostro sia laser a colori.
Possibile che l'affare sia reale? Siamo certi che non ci sia qualcosa sotto? Ecco come, nel corso degli anni, HP e i suoi amici/concorrenti, si sono adoperati per renderci tutti inconsapevoli schiavi dei loro prodotti.

:: Lo specchietto per le allodole

Oggi con meno di 100 euro, in alcuni casi si risparmia ancora, possiamo portare a casa una stampante di buona qualità che reputiamo più che adatta per i nostri scopi. Addirittura, con qualcosa in più, possiamo permetterci anche una laser a colori. Installiamo il tutto, i driver e il software che viene fornito insieme alla periferica, facciamo un po' di prove e andiamo avanti a usare la nostra nuova stampante per qualche tempo, fino a quando una spia lampeggiante o un messaggio sul monitor non ci dice che sta per finire la cartuccia dell'inchiostro. E qui casca l'asino (noi): la cartuccia dell'inchiostro costa almeno un terzo dell'intera stampante, se non di più. Di solito poi le stampanti montano due cartucce distinte, una per il nero e una per i colori, e se facciamo due conti ci rendiamo presto conto che, quasi quasi, ci conviene comprare una nuova stampante invece di comprare nuove cartucce. E, da quel momento, saremo diventati schiavi di HP (o qualunque altra marca, fa lo stesso): se vogliamo i risultati migliori, ci accorgeremo che dovremo comprare sempre cartucce e carta originali.

:: Il miraggio delle laser

Ammettiamo anche che tutto sommato la cosa ci stia bene, tanto, per quello che stampiamo, ci sta bene pure comprare solo materiale originale una volta all'anno. Così, se abbiamo scelto di comprare una laser a colori, che troneggia da un



La cartuccia di ricambio spesso costa spropositatamente, anche più di un terzo della stampante stessa.

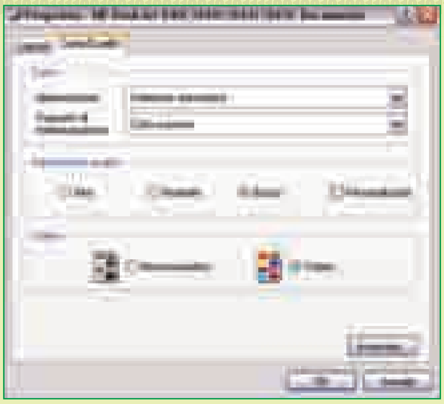
annetto sulla nostra scrivania come un pezzo pregiato, ci siamo accontentati di comprare il suo toner originale, costoso sì ma comunque conveniente. Ad un certo punto strani rumori che provengono dalla stampante ci mettono in allarme: le stampe non escono più perfette e troviamo macchie di vario genere, i fogli si incastrano sempre più spesso tra i rulli e, disperati, non possiamo fare altro che constatare l'insorgere di un problema e rivolgerci all'assistenza. Tanto è in garanzia, pensiamo, l'abbiamo comprata meno di un anno fa. E qui giunge la batosta: l'assistenza ci informa che il gruppo stampa (il tamburo, o come lo vogliono definire) è da sostituire, e che la sostituzione costa quasi come la stampante nuova. Diamine, è in garanzia no? Leggiamo sempre i manuali di istruzioni, anche nelle pagine finali dopo aver installato il tutto, è lì che spesso si nasconde l'inghippo. Il gruppo stampa di una laser è "materiale di consumo", considerato alla stessa stregua del toner, e quindi non è coperto dalla garanzia. Vogliamo continuare a usare la nostra laser? Dobbiamo spendere 3/4 del suo costo per comprare un gruppo stampa nuovo, volenti o nolenti. Di nuovo schiavi di HP (il discorso vale ancora per tutte le marche).

:: Inutile parsimonia

Dopo esserci amaramente accorti che la nostra stampantina economica in realtà non è economica per niente, iniziamo a pensare come fare per risparmiare il più possibile sull'inchiostro. Ci accorgiamo quindi che è possibile stampare in modalità bozza, almeno per le cose meno importanti, e che la cosa che stampiamo più spesso è del semplice testo, quindi ci viene logico pensare che, stampando solo in bianco e nero e in modalità bozza, le cartucce possano durare di più. Poveri illusi. Primo: ad HP non interessa farci risparmiare, anzi, siamo le mucche da mungere (ovviamente per soldi, non per latte) e da allevare come tali. Ci accorgeremo quindi che non riusciamo a stampare a risoluzioni inferiori a 600x600 (quando per una bozza di testo già 300x300 sono tanti) e che, un bel giorno, la cartuccia semplicemente si rifiuterà di funzionare e la stampante ci dirà di sostituirla per forza. Un chip, un minuscolo chip contenente una



Anche per le laser troviamo l'inghippo: il gruppo stampa è considerato materiale di consumo e quindi non è coperto da garanzia.



Nel pannello di controllo della stampante, richiamato dal driver, possiamo impostare la qualità di stampa, ma non sempre questo ci fa risparmiare.

data di scadenza, oltre la quale la cartuccia non può essere più utilizzata. Ecco la sorpresa che ci viene riservata. E non è l'unica: molte stampanti a basso prezzo non ci permettono nemmeno di stampare in bianco e nero, possiamo ottenere il nero solo come combinazione degli altri colori e del nero stesso, sprecando grandi quantità d'inchiostro.

:: Qualche soluzione?

Il nostro obiettivo è quello di ridurre al minimo il costo per pagina delle nostre stampe e di "sbloccare" alcune funzioni della stampante, magari presenti in modelli superiori e presenti, ma bloccate, in quelli inferiori. Non si tratta di obiettivi che si raggiungono con poco sforzo o modificando qualche chiave di registro: spesso sono richieste buone conoscenze dell'hardware e del software, buone capacità di programmazione e, soprattutto, tempo ed esperienza. Tuttavia nulla è impossibile. Tanto dipende anche dal modello di stampante: spesso certe procedure funzionano perfettamente con stampanti non nuovissime, ma sono del tutto inutili con quelle attuali. L'inizio è comunque un'approfondita ricerca sul Web, magari aprendo la stampante per scovare sigle di chip e caratteristiche hardware, e "rapinando" a mani basse le aree per gli sviluppatori dei siti dei produttori.



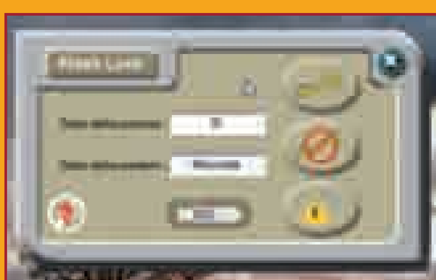
Chiavi imbattibili

Le chiavette dotate di software di crittografia sono sempre più diffuse ma è sicuro affidargli i nostri segreti? Abbiamo messo la TDK Trans-It sotto attacco

Le chiavette USB hanno cambiato il modo in cui vengono conservati i dati, sia aziendali che personali. Dopo chiavette su cui trasferire tutti i nostri dati, chiavette che si convertono in lettori MP3, chiavette capaci di ospitare centinaia di programmi funzionanti senza installazione e altre chiavette che contengono interi sistemi operativi autonomi, ecco arrivato il momento delle chiavette USB crittografate.

:: Sicure son sicure

Un paio di anni fa, questi dispositivi erano ancora sperimentali e ogni costruttore proponeva le proprie tecniche di cifratura. Nella maggior parte dei casi, le chiavette di questo genere erano dispositivi USB compositi, con una sotto chiave in chiaro e una sotto chiave cifrata e accessibile solo opportuna decifratura tramite un software dedicato. Questa strada, tuttavia, rappresentava un vicolo cieco: il doppio hardware rendeva la chiavetta molto più costosa, offrendo il mercato a sistemi di cifratura software, disponibili anche gratuitamente. Inoltre le chiavette non potevano essere aggiornate nel caso venissero identificati metodi di accesso ai dati protetti, rendendo diffidenti gli acquirenti. Per finire, la netta separazione non permetteva agli utenti di sfruttare tutta la capacità per un unico scopo, costringendo gli utenti a dividere i propri dati in due. Negli ultimi tempi, invece, si è assistita a una svolta: la memoria della chiavetta non viene più divisa in due entità separate ma l'intero sistema viene gestito da un software che accede a un chip in grado di supportare l'utente nelle funzioni di cifratura. Tra le chiavette appena uscite ci sono le TDK Trans-It, disponibili con tagli da 2 a 16 Gb, che sfruttano al massimo questo nuovo tipo di approccio. L'abbiamo presa, analizzata a fondo fino a smontarla e... "distruggerla"; ecco il risultato.

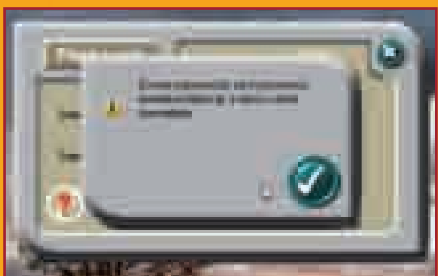


Flash Lock sembra un programma di crittografia ma è solo un'interfaccia con il chip interno della chiavetta USB. Proprio per questo motivo sembra piuttosto lento nel funzionamento.

:: Come funziona

Anch'essa utilizza il sistema del chip; lo scopo è quello di rende più elastica la gestione della memoria, permettendo agli utenti interessati di cifrarla completamente e agli altri di ignorare questa caratteristica. Il programma di codifica viene ospitato nella parte libera della memoria della chiavetta USB, così da essere sempre attivabile per permettere l'accesso alla parte cifrata.

Il meccanismo di funzionamento prevede che si avvii il programma, si indichi una password di accesso all'area cifrata e si specifichi quanto spazio sulla chiavetta riservargli. Il software programmerà la chiavetta USB in modo da nascondere o mostrare le partizioni cifrate e provvederà a far identificare da Windows le aree interessate. Nel caso in cui si tentasse l'accesso alla parte cifrata sbagliando troppe volte la password, come in altri modelli, sono previsti meccanismi di auto distruzione dei dati.



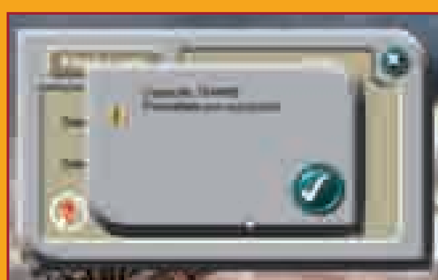
L'avviso è abbastanza chiaro: un altro errore e il disco, cifrato, sparirà nel nulla. L'operazione è svolta dall'hardware della chiavetta, non da Windows.

:: Sconfitta

Guardando alle funzioni del software, quindi, sembra del tutto impossibile riuscire a recuperare i dati da una partizione cifrata con sistemi moderni. Dal punto di vista della cifratura è persino impossibile un'analisi: la zona cifrata è un messaggio a chiave simmetrica, AES a 256 bit, a singolo utilizzo. In pratica, le uniche tecniche che potrebbero rompere il livello di sicurezza sono la forzatura del software o il brute force crack della password. La prima possibilità, però, è negata a causa del fatto che la codifica è hardware. Il programma di cifratura non conserva la password e nemmeno si occupa di variare la visibilità delle partizioni della chiavetta. Il suo scopo è quello di mera interfaccia tra l'hardware di gestione della chiavetta e l'utente. La tecnica del brute force, invece, non può nemmeno essere tentata visto che è proprio l'hardware della chiavetta a cancellare i dati in caso di errati inserimenti della password. A nulla vale persino il tentare di riportare a zero il numero di tentativi fatti: è un valore che viene registrato dal chip di controllo e non viene scritto in alcuna zona della chiavetta e l'incremento avviene tramite firmware della chiavetta stessa, non tramite software. C'è di più perché persino le tecniche di acquisizione forensi non possono nulla contro questa tecnologia: l'area di memoria che ospita la parte cifrata è di fatto resa invisibile e inaccessibile dall'hardware della chiavetta e non è nascosta nella parte visibile. Questo significa che dedicando 4 Gb alla cifratura, senza la password opportuna, una chiavetta da 8 Gb sarà vista come una da 4 e solo la scritta sulla chiavetta stessa indicherà la sua capacità reale. Viste le condizioni poste dall'analisi, l'unico metodo possibile per recuperare almeno l'area cifrata senza farla distruggere dal sistema è quella di operare a livello hardware, aprendo fisicamente la chiavetta ed affidandosi a metodi di analisi decisamente invasivi. Peccato che, in questo modo, sarà piuttosto facile distruggere la chiavetta invece che recuperarla e solo pochi laboratori specializzati sono in grado di svolgere questi compiti.



Piccola, blu translucido, la nuova Trans-It è disponibile in tagli da 2 a 8 Gb e contiene un chip di crittografia decisamente sicuro.



Fine dei dati cifrati. Piuttosto di rompere la sicurezza, le informazioni vengono distrutte. Una strategia ottima ma che può creare problemi a molti utenti.

:: Troppo sicura? Non tanto...

Se è vero che, diversamente da altri sistemi di archiviazione, persino la speranza di recupero legittimo tramite brute force o usando sequenze di password probabili è destinato a fallire, è anche vero che il recupero può essere semplificato se illegittimo in quanto il conteggio degli errori viene resettato ogni volta che viene azzeccata la password.



Persino l'uso di hardware forensi, capaci di intercettare il traffico dati USB è inutile: basta il tentativo di decifratura per attivare le caratteristiche della chiavetta.

Questo significa che è possibile prendere la chiavetta di un soggetto, fare qualche tentativo e rimetterla al suo posto in attesa che lui la utilizzi per poi ripetere il tentativo. L'unico modo per proteggersi, per lui, sarebbe quello di cambiare la password ogni volta. Anche qui, però, anche l'utente più prudente potrebbe essere battuto: un keylogger hardware costa pochi euro e non può essere identificato da alcun software. Come al solito, il problema sta nella quantità di paranoia posseduta dall'utente che usa il sistema, non dalle capacità tecniche dello stesso.

SPQH (Sono Pazzi Questi Hacker)

Che "hacker" non significhi solo il classico smanettone lo sappiamo bene: fin dove possono arrivare lo scopriamo in queste pagine

Quando si parla di hacker, subito il pensiero vola alla tastiera del PC e a interminabili notti davanti al monitor per tentare di entrare in qualche rete privata o simili. Ma hacker è molto più di questo: è anche l'essere curioso di natura, voler capire come funzionano le cose, e chi capito questo riesce ad adattarle per altri scopi ed esigenze. E non è detto che queste cose debbano essere per forza indispensabili o abbiano uno scopo ben preciso, alla fine l'importante è anche divertirsi. Perché gli hacker, spesso, sono fuori di testa!

:: La culla robotizzata

Non è un vero e proprio aggeggio "hacker", ma niente che un hacker non riesca a mettere insieme da solo. All'apparenza è un normale lettino in legno per il bebè, ma non appena un sensore si rende conto che il bimbo piange, la culla inizia a muoversi da sola avanti e indietro a un ritmo che, a detta del costruttore, è pari a quello del battito cardiaco del genitore. Il problema è il costo: questo lettino può essere affittato per 100 dollari al mese, oppure comprato per 5000 dollari. Volendo passare all'autocostruzione, un hacker con il pallino della falegnameria sicuramente lo realizzerebbe con molto meno! In sostanza, si tratta di un sensore collegato a un micro controller di qualche tipo, programmato per riconoscere il pianto e attuare, mediante motori elettrici, delle ruote poste sotto il lettino o altro meccanismo analogo.



Il punto più difficile dovrebbe essere la programmazione del micro controller, ma comunque niente che un hacker non riesca a risolvere egregiamente.



Cosa c'è di meglio di una culla-robot per riuscire a dormire la notte anche se il bebè si mette a piangere?

:: Lo snack è video-servito!

E mentre il bebè dorme e il papà hacker non deve più preoccuparsene, cosa c'è di meglio di uno spuntino davanti al PC? Ecco quindi il tostapane VHS... O il VHS tostapane, come vogliamo definirlo. Prendiamo un vecchio tostapane, ne smontiamo resistenze e meccaniche varie, montiamo il tutto nel case di un vecchio videoregistratore e in pochi minuti avremo pane tostato direttamente nel piatto, posto che riusciamo a metterlo alla giusta distanza.
Hack come questo, ricordiamocelo, richiedono attenzione e cura nella realizzazione, dato che è molto facile sbagliare qualcosa e rischiare di dare fuoco alla casa. Soprattutto ricordiamoci che le piastre del tostapane scaldano parecchio, quindi devono essere adeguatamente ventilate e schermate dalla struttura del videoregistratore, che di solito è in plastica: potrebbe fondersi in un attimo, e addio spuntino.



Il vecchio videoregistratore è morto? Resuscitiamolo metafisicamente in un tostapane per uno spuntino davanti al PC.

:: Stephanie

Questo hack ha dell'incredibile: una maschera di plastica, simile a quelle usate nei costumi per le feste o per carnevale, trasformata in un avatar per la nostra stanza. Che cosa fa un avatar? Di solito nulla, finché non glielo chiediamo chiaramente. Stephanie, infatti, reagisce a comandi vocali impartiti dall'hacker che l'ha costruita, ed è in grado di accendere luci, chiudere le veneziane alle finestre ed è anche in grado di rispondere verbalmente.Il tutto si basa sulle librerie SAPI di Microsoft, un insieme di funzioni per il riconoscimento vocale e per la lettura automatica del testo. Grazie a queste librerie, Stephanie riconosce il proprio nome ed è in grado di riconoscere e obbedire a semplici comandi, proprio come spegnere o accendere la luce. Per darle un minimo di animazione, l'autore ha tagliato la maschera in maniera adeguata e ha creato un semplice animatronic per il movimento della bocca mentre Stephanie parla. Assolutamente da avere accanto ai nostri PC!



Niente più solitarie notti davanti al computer: Stephanie terrà compagnia all'hacker che l'ha costruita e lo aiuterà in semplici azioni nella sua stanza.

:: Sputafuoco.. e acqua!

In questa categoria troviamo numerosi articoli, dato che ogni hacker che si rispetti è anche un burlone e (soprattutto) giocatore di giochi di ruolo/Doom/sparatutto, e che ovviamente voglia essere sempre "armato" a dovere. Abbiamo quindi una stupenda doppia mitragliatrice per proiettili di inchiostro, in grado di sparare ben 34 colpi al secondo. Se l'inchiostro non ci sta bene, possiamo sempre passare alle palline da ping-pong: un robot che a ritmo di musica è in grado di spararle alla velocità di 170 miglia all'ora, ben 273 Km/h! A questa velocità fanno male anche quelle, meglio rimanere fuori portata. Possiamo quindi ripiegare verso qualcosa di più inoffensivo, e magari più divertente: che ne dite di un cannoncino ad acqua per fare uno scherzo agli amici? Lo possiamo pilotare via USB ed è comandato da un micro controller, oltre a essere divertente può essere anche molto istruttivo se ci interessa imparare come funzionano questi componenti.



Minacciosa, ma innocua: spara proiettili di inchiostro a un rate di ben 34 colpi al secondo.



Meno minacciosa e più divertente, una realizzazione che via USB e micro controller spruzza acqua in faccia ai nostri amici.

:: Micromotori

Con i micromotori che generano la vibrazione nei cercapersone si possono fare cose molto interessanti. Per esempio, possiamo montarli su una cintura (sì, proprio quella che infiliamo nei jeans) e, pilotati da un modulo bussola elettronico tipo quelli installati in navigatori e altri dispositivi simili, ci indicheranno sempre il nord facendoci tremare le braghe.Se poi ce ne avanza uno, possiamo costruire anche un micro robot usando la testa di uno spazzolino da denti, una batteria a bottone e una striscia di biadesivo: non potremo controllarlo, ma sarà divertente vederlo scorazzare per il tavolo!

Ovvero: come riescono ad avvelenarci col cibo malgrado tutto





Rimarremmo allibiti sapendo con precisione quanti prodotti hanno solo aromi chimici alla fragola e non fragole vere...

Sentirlo al telegiornale o leggerlo sul Web (anche grazie a Fravia+, "apritore d'occhi" per molti) fa sempre storcere la bocca, ma alla fine ci caschiamo sempre, come se fosse più forte di noi. Compriamo alimenti non solo perché è necessario per sopravvivere, ma anche perché è un modo per autogratificarci col piacere del cibo. Il guaio è che spesso non abbiamo proprio idea di cosa stiamo mandando giù: apriamo la confezione della merendina istintivamente, mangiamo il contenuto senza pensarci e non ci prendiamo la briga di leggere quanto scritto nella lista degli ingredienti.



:: Altro che Star Trek

Vita facile, nel Ventiquattresimo Secolo: se ho fame, mi avvicino al replicatore del mio alloggio, chiedo quello che voglio e, dopo qualche scintilla e un effetto audio degno del miglior sintetizzatore, pesco il piatto dal comparto e mi metto a mangiare. Ma da dove viene quello che ho nel piatto? In una nave stellare del futuro, per grande che sia, le risorse non possono essere infinite. Dato che i replicatori, per l'appunto, "replicano" un cibo ma non è di certo cibo fresco, è facile supporre che in qualche maniera esso venga sintetizzato a partire da molecole costruite alla bisogna. Non c'è vero succo di prugna nel bicchiere di Worf, e nemmeno gelato al cioccolato per Troy, ma una bevanda al gusto di prugna e un dessert al gusto cioccolato, rispettivamente. Vi starete chiedendo, ma questo che ha a che fare con ciò che mangiamo oggi?

In molti casi, la realtà non è molto distante dalla fantasia. Pensiamo per esempio a quanti prodotti possono essere realizzati con le fragole: le possiamo consumare fresche o possiamo trovarle in marmellate, torte, gelati, sciroppi, gelatine, caramelle e chi più ne ha più ne metta. Ma siamo certi che la produzione mondiale di fragole sia sufficiente per coprire la domanda di questo prodotto? La risposta, facile da intuire, è che non lo è per niente. Anzi, si calcola



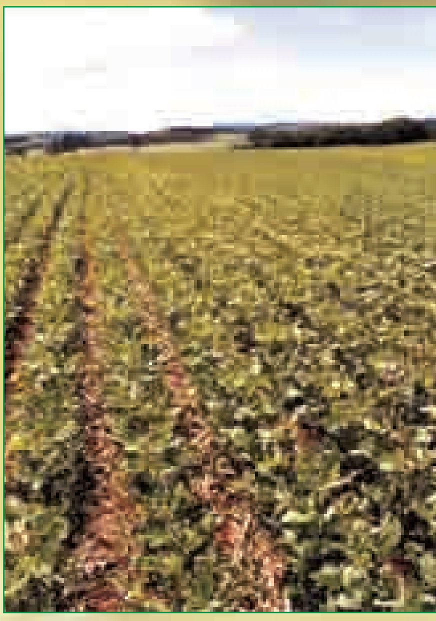
che le fragole fresche prodotte mediamente da un Paese non bastino che per meno del 10% del fabbisogno dello stesso Paese, considerando tutti i prodotti in cui si presume di trovarle. Come si faccia a sopperire al restante 90% rimane un fatto oscuro per la maggior parte dei consumatori. Aromi, ecco cosa sopperisce. Ma non si tratta di aromi derivati da vere fragole: sono aromi sintetici, cioè prodotti chimici che ricreano con buona approssimazione il gusto di fragola. Ciò che è peggio è che la legislazione in materia, nell'ambito della Comunità Europea, permette di indicare tutti questi composti semplicemente con la parola "aromi", senza alcuna specificazione.

:: Al rogo gli OGM!

Tutti fuggono al cospetto degli OGM, anatema sulle aziende che operano nel settore e che vogliono avvelenarci! Poi compriamo biscotti e gelati a base di soia, fanno anche bene alla salute perché contribuiscono a non alzare il livello di colesterolo. Non si fa caso però che quasi la metà delle colture di soia di tutto il mondo è modificata geneticamente, e la soia oggi la troviamo praticamente in tutto. Sì, anche nella crema alla fragola che tanto ci piace, insieme agli aromi che simulano il sapore e il profumo di fragole vere. A questo punto è lecito chiedersi fino a che punto siamo coerenti con noi stessi, e forse è il caso anche di stare più attenti e di informarci meglio su quanto contenuto nei cibi.
Se poi vogliamo fare i puristi a tutti i costi, non dovremmo mangiare più niente: la soia è tra i componenti principali di molti mangimi dati come nutrimento agli animali, quindi in un modo o nell'altro rischiamo di ingerirne una buona quantità, volenti o nolenti. E non andiamo a spulciare tra i prodotti usati in ristoranti, fast food e chioschi vari. Meglio non sapere...

:: La moda del BIO

Da quando qualcuno ha iniziato a gridare a gran voce contro gli avvelenamenti lenti e inesorabili che le industrie alimentari ci propinano col cibo che ingeriamo, è nata quella che non si può definire altrimenti che come moda del BIO. Diciamocelo, tutto ciò che oggi viene definito BIO è semplicemente una trappola commerciale che, oltre alla beffa, aggiunge il danno. Il "prodotto da agricoltura biologica" dovrebbe essere un prodotto coltivato con metodi che non impieghino sostanze pericolose (ma sarebbe meglio dire semplicemente vietate dalle direttive europee, perché molte sostanze in sé pericolose passano comunque il vaglio del BIO), il che, sorpresa sorpresa, è esattamente come il buon senso ci dice che debba essere coltivato o prodotto un alimento destinato alle persone. La differenza è che questi prodotti marchiati BIO li paghiamo dal 10 al 20% in più dello stesso prodotto ottenuto invece con metodi "tradizionali", cioè con le procedure, i fertilizzanti e gli antiparassitari usati per decenni dalle agricolture di tutto il mondo fintanto che nessuno si lamentava della pericolosità di certe sostanze. In pratica, paghiamo di più per avere un cibo ottenuto così come dovrebbe essere. Questo grazie, naturalmente, all'anima commerciale che ormai comanda e guida tutto ciò che facciamo nella nostra vita: il fine ultimo è e rimane sempre il profitto e non la salute, come è nelle migliori tradizioni Ferengi.



La quasi totalità della soia contenuta nei cibi è geneticamente modificata, e questo non è un dato indicato sulle etichette.

:: Per trovare informazioni

Abbiamo trovato in rete un utile opuscoletto prodotto dall'Unione Nazionale Consumatori insieme alla Fondazione Monte dei Paschi di Siena. Si tratta di un documento PDF che troviamo all'indirizzo http://www.consumatori.it/index.php?option=com_content&task=view&id=435&Itemid=409 e che spiega, in termini semplici e abbastanza esaurienti, come leggere le etichette dei cibi che quotidianamente compriamo al supermercato.

Comprando prodotti BIO spendiamo di più per avere quello che dovrebbe essere la normalità. E non tutto è veramente "bio".



I SEGRETI DEI SERIAL NUMBERS

Dovrebbero proteggere i software dalla copia indiscriminata. Lo fanno davvero?

Una cosa è certa: non esiste un metodo unico e affidabile per creare un sistema di protezione del software; ne è prova il "fiorente mercato" della pirateria, tutto fuorché debellata anche usando i sistemi più complessi. Il sistema a codice seriale è stato uno dei primi a essere ideato e implementato, ma anche uno dei primi a essere craccato da chi disponeva di software e conoscenza adeguata. Ma andiamo con ordine.

:: Come funziona

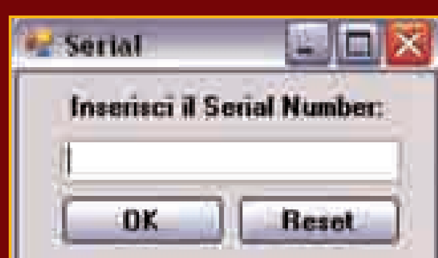
Ognuno di noi ha dovuto, prima o poi, inserire un codice seriale per attivare un programma appena installato sul PC. In genere, il seriale viene fornito dal produttore dopo aver ricevuto notifica del pagamento avvenuto, spesso a stretto giro di e-mail. A noi non resta che riportarlo in un'apposita casella, fare clic su un pulsante e, magicamente, l'applicazione diventa registrata, mettendoci a disposizione anche quelle funzioni che erano disabilitate nella versione demo o shareware. Dal lato software, il codice seriale inserito deve essere validato in qualche modo. Deve esistere quindi una procedura, nel programma, in grado di leggere il contenuto della casella, comparare il codice inserito con un codice valido e comportarsi poi in maniera adeguata: se il codice non è valido, ce lo comunica e non cambia niente, se invece è valido scriverà qualcosa in una chiave del registro o in un file di configurazione del programma perché questo, in futuro, sappia che è stato registrato con successo.

Questo ovviamente è uno schema di base, che nel corso degli anni è stato adattato, modificato e addirittura stravolto per cercare soluzioni sempre diverse e nuove e tentare così di limitare i danni causati dai crackers, ma sempre con la stessa filosofia di fondo.

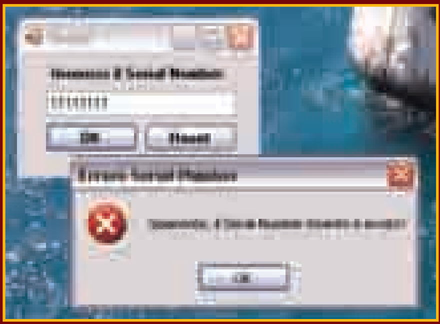
:: Un po' di codice

Proviamo a scrivere un semplice programmino il cui unico scopo è controllare la validità di un serial number. È un'occasione anche per provare sul campo Visual Studio 2008 Express Edition, di cui abbiamo parlato in questo stesso numero. Innanzitutto creiamo un nuovo progetto per la nostra applicazione: si chiamerà **Serial** e sarà di tipo **Applicazione Windows Form** (è nella categoria **Visual C++/CLR**). L'ambiente di sviluppo ci mette a disposizione la finestra principale della nostra applicazione, su cui andremo a porre gli elementi per l'interazione. Questi elementi sono quattro: una label che contiene il messaggio "Inserisci il Serial Number:", una casella di testo per l'inserimento e due pulsanti, uno ("OK") per la conferma del codice inserito e uno ("Reset") per svuotare la casella di testo.

Iniziamo a modificare le proprietà dei diversi elementi: per l'etichetta



La finestra principale dell'applicazione di prova: è molto semplice da creare grazie a Visual Studio 2008 Express Edition.



Il codice è sbagliato: dobbiamo quindi tornare indietro e riprovare.

label1 dobbiamo modificare solo la proprietà **Text** inserendo il testo indicato. Per la casella di testo **textBox1** diamo il valore 8 a **MaxLength**, per forzare il codice seriale a un massimo di 8 cifre. Il primo pulsante, **button1**, avrà **Text** impostata a "OK", mentre **button2** a "Reset". Possiamo dire che il lavoro di preparazione dell'interfaccia termina qui, ora si passa al codice. Nel pannello in cui abbiamo costruito l'interfaccia, facciamo prima doppio clic sul pulsante OK e poi sul pulsante Reset: in questo modo aggiungeremo i template per le procedure di gestione eventi di questi pulsanti. Passiamo alla visualizzazione del codice e modifichiamole come da **Codice1**.

In questo caso, il più semplice nel caso dei numeri seriali, quello valido è integrato direttamente nel codice dell'applicazione ed è uguale a **12345678**. Compiliamo il progetto ed eseguiamolo con **Ctrl+F5** (se non l'abbiamo già compilato Visual Studio ci chiederà se desideriamo farlo). Vediamo cosa succede se inseriamo un codice sbagliato, per esempio **78978978**: l'applicazione risponde con un messaggio che ci avvisa che abbiamo sbagliato.

Se invece il codice inserito è corretto, il messaggio mostrato confermerà la validità del numero.

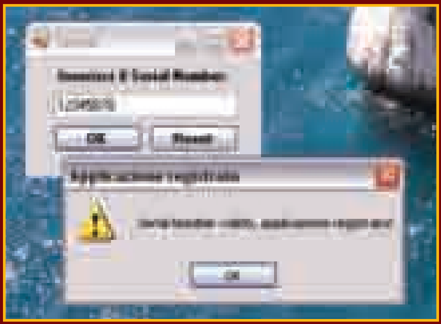
:: Il punto debole

È facile intuire che una protezione di questo tipo in realtà non protegge alcunché: basta dare una sbirciata all'eseguibile del programma con un visualizzatore di file binari per scovarlo e usarlo per craccare l'applicazione. In realtà è difficile che un cracker si passi tutto l'eseguibile di una applicazione alla ricerca di un codice valido, esistono altri strumenti molto più validi che lo aiutano nell'operazione, come un buon debugger; tuttavia il punto è che un sistema di

```
[Codice 1]
private: System::Void button1_Click(System::Object^  sender, System::EventArgs^  e) {
        if (Serial::Form1::textBox1->Text == "12345678") {
                MessageBox::Show("Serial Number valido, applicazione registrata!",
"Applicazione registrata", MessageBoxButtons::OK, MessageBoxIcon::Exclamation);

// Inserire qui il codice che scrive nel registro o nel file .ini la registrazione del
programma.

        } else {
                MessageBox::Show("Spiacente, il Serial Number inserito è errato!",
"Errore Serial Number", MessageBoxButtons::OK, MessageBoxIcon::Error);
        }
}
private: System::Void button2_Click(System::Object^  sender, System::EventArgs^  e) {
        Serial::Form1::textBox1->Text = "";
}
```



Ora il codice seriale è corretto e la nostra applicazione risulta registrata.

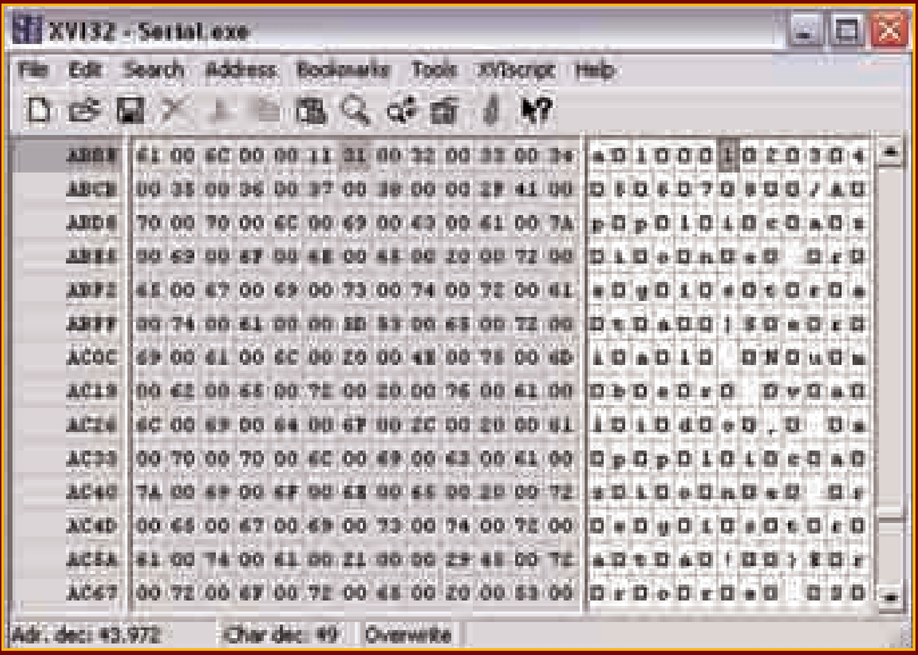
protezione di questo tipo è davvero troppo debole, e tanto vale non implementarlo nemmeno.

Una possibile soluzione quindi è quella di non inserire per niente il seriale nel codice del programma, men che meno se è in chiaro. L'alternativa migliore è calcolarlo al momento, in modo che sia presente solo in memoria e non sia possibile quindi risalire in chiaro a un numero seriale valido.

:: Il calcolo del codice

Naturalmente si tratta sempre di esempi, che vanno adattati di volta in volta alle proprie esigenze. Va però sempre tenuto presente che con metodi di protezione di questo tipo faremmo prima a rendere Open Source il nostro programma, più utile che proteggerlo con uno scudo spesso come un foglio di carta velina. Per prima cosa, la nostra routine dovrà calcolare un serial number valido. L'algoritmo non è standard e qui davvero possiamo sbizzarrirci: tuttavia la base di calcolo deve essere qualcosa di conosciuto a priori sia dal programmatore sia dall'utente. I casi che si presentano sono quindi due: o si usa un dato che sta sul PC del programmatore, e in questo caso deve essere incluso nel codice del software, o si usa un dato che sta sul PC dell'utente, che deve quindi essere trasmesso in qualche modo al programmatore per il controllo.

Nel primo caso, il programmatore include una base di partenza (seed) nel proprio codice. Al momento del controllo del serial number in-



Eccolo! Con un editor esadecimale basta aprire l'eseguibile del programma per scovare il seriale corretto che è stato maldestramente inserito in chiaro dal programmatore.

serito, la routine calcola ex novo un codice seriale a partire da tale base e lo confronta con quello inserito dall'utente. È il sistema standard usato per esempio nelle applicazioni shareware, in cui non si ha controllo sulla diffusione del software fino a quando un utente non decide di registrarlo (usualmente via e-mail). Nel secondo caso, il software calcola un codice intermedio a partire da un dato presente sul PC dell'utente (per esempio basato sulla configurazione hardware). Questo codice deve essere trasmesso al programmatore, che lo usa per generare il serial number finale valido e lo trasmette all'utente per la registrazione. Questo secondo metodo ha il vantaggio di rendere il seriale ottenuto strettamente legato alla macchina su cui si installa il software, che quindi non funzionerà su altri PC (è il sistema usato da Windows).

:: Numeri fragili

Un sistema di protezione come questo è molto debole, e rischia di durare il tempo di un buon film: va benissimo per scoraggiare il "cracker occasionale", ma non quello esperto e risoluto. La debolezza sta nel fatto che, in una maniera o nell'altra, la procedura per il calcolo del numero seriale deve essere inserita nel codice del software. Questo vuol dire anche offrirla sul piatto d'argento per un cracker con gli strumenti giusti: basta Soft-ICE e un pizzico di conoscenza di come funzionano le cose in Windows e la nostra protezione non solo durerà poco, ma darà modo anche al malintenzionato di creare un keygen usando il nostro stesso codice.

Gli basta infatti individuare dove, nel nostro programma, viene calcolato il seriale valido e comparato con quello inserito dall'utente per avere due scelte a disposizione: far saltare il controllo comparativo (del tipo "se è diverso salta a codice errato" a "in qualunque caso salta a codice valido"), oppure estrapolare la routine, scrivere un programmino che la includa e avere a disposizione tutti i codici seriali desiderati.



Soft-ICE, uno tra gli strumenti più amati dai crackers, permette di scovare una routine di calcolo di un serial in poco tempo: basta seguire il flusso del programma.

:: Rafforziamoli

Dovremo fare un po' di ricerche sul Web, documentarci bene e studiare molto, ma ci sono delle tecniche che permettono di adottare una protezione a codice seriale un po' più stagna di quelle viste finora. Innanzitutto, possiamo adottare qualche tecnica anti-debugger: inserendo in punti adatti dei trap per l'interrupt 03h, quello usato appunto dai debugger per impostare i loro breakpoint, potremo evitare che qualcuno guardi nel nostro codice mentre il programma è in esecuzione. Non è nemmeno questa una tecnica infallibile, ma contribuirà a ridurre ulteriormente le possibilità che qualcuno cracchi la nostra applicazione. Vincoliamo poi il seriale all'hardware come fa Windows: un programma su ogni computer e solo su quello, così il seriale, anche se individuato, non funzionerà su altri PC (ma può sempre essere ricalcolato dall'hacker). Usiamo un po' la fantasia: essere prevedibili è il principale nemico di ogni programmatore che vuole proteggere la propria opera.

CREA IL TUO SITO DI
HACKER JOURNAL



Realizza il sito di Hacker Journal così come lo vorresti, pubblicalo in un area non indicizzata del tuo spazio Web e inviaci il link.

I migliori cinque, a insindacabile giudizio della redazione, verranno presentati nella home page di hackerjournal.it dove i lettori potranno votare ed eleggere il primo classificato.

Il sito vincitore verrà utilizzato, interamente, o esculsivamente come template grafica, come sito ufficiale di Hacker Journal.

Invia una mail all'indirizzo sito@hackerjournal.it con il link per visualizzarlo, i tuoi dati e una dichiarazione liberatoria di utilizzo.

www.hackerjournal.it

Virtual Machine: impariamo a scegliere



Microsoft, VmWare e pochi altri puntano molto sulla virtualizzazione, spacciandola come il futuro dell'IT

Di sistemi di virtualizzazione, oggi, ce ne sono molti, sia a pagamento che gratuiti. Se alcuni scelgono l'uno o l'altro per la fiducia accordata al produttore, in molti casi sembra che tutti si equivalgano e non sia possibile identificare il migliore o quello che offre i maggiori vantaggi. In realtà, tra gli oltre 60 sistemi disponibili, alcuni funzionano solo su determinate architetture, altri sono incompleti, altri ancora non hanno un'elevata affidabilità per certi compiti.

:: Per tutti o per nessuno

Se siamo alla ricerca di un sistema di virtualizzazione che possa funzionare con qualsiasi sistema operativo host e far funzionare qualsiasi guest, per esempio, ci si può rivolgere a Bochs, bochs.sourceforge.net. Sviluppato per semplificare la vita agli sviluppatori di sistemi operativi, è a tutti gli effetti un vero e proprio emulatore di piattaforma x86 open source. Può emulare senza difficoltà i processori dal 386 agli ultimi a 64 bit, così come può far funzionare dal vecchio DOS a qualsiasi versione di Linux o di Windows Vista.

Purtroppo, Bochs è tutt'altro che diffuso proprio a causa della sua grande adattabilità: come tutti gli emulatori puri, non ottimizza il codice del sistema guest e risulta decisamente lento. Riuscire a far funzionare con profitto la maggior parte dei programmi nei sistemi guest è del tutto impossibile. In generale, per avere buone prestazioni, occorre rivolgersi a sistemi più specializzati. Tra tutti, il più famoso è senz'altro VMWare che, in realtà, non è un unico sistema ma un insieme di piattaforme di virtualizzazione con differenti caratteristiche. Si va da VMWare Workstation, adatto a un utilizzo saltuario, fino ad arrivare a VMWare ESX Server: un sistema di virtualizzazione che non necessita di sistema operativo host e che è studiato per le grandi infrastrutture.

Quest'ultimo, attualmente, è il non plus ultra della virtualizzazione: un sistema operativo dedicato a questo scopo e che permette di sfruttare al massimo l'hardware più potente oggi in commercio. Ovviamente le sue caratteristiche sono del tutto particolari, come la possibilità di spostare una macchina virtuale da un server a un altro senza fargli perdere nemmeno le connessioni di rete in corso, ma anche il suo costo è qualcosa che col-

I SISTEMI DISPONIBILI

Nome	Produttore	Host CPU	Guest CPU	OS Host
Bochs	Kevin Lawton	Qualsiasi	x86, AMD64	Windows, Windows Mobile, Linux, IRIX, AIX e altri
Containers	Sun Microsystems	x86, x86-64, SPARC (portabile)	come l'host	Solaris 10
DOSBox	Peter Veenstra and Sjoerd	Qualsiasi	x86	Linux, Windows, Mac OS X, BeOS, Solaris, AmigaOS, altri
DOSEMU	Progetto comunitario	x86, AMD64	x86	Linux
GXemul	Anders Gavare	Qualsiasi	ARM, MIPS, M88K,	Unix-like
KVM	Qumranet	X86 con virtualizzazione, IA64,s390,PowerPC	come l'host	Linux
Linux- VServer	Progetto comunitario	x86, AMD64, IA-64, Alpha, PowerPC/64 e altri	come l'host	Linux
LynxSecure	LynuxWorks	x86, Intel VT-x, Intel VT-d	x86	Nessuno (h

pisce: la licenza di base, per un anno, per una macchina con 2 processori, costa oltre mille euro. Che vanno aumentati per poter sfruttare le caratteristiche del sistema, visto che una macchina singola a due processori serve a poco come macchina da virtualizzazione. A cui aggiungere, naturalmente, i costi dell'hardware e quelli di licenza dei sistemi operativi host. Se vogliamo procedere per gradi, però, meglio iniziare usando VMWare Server 2 che ha caratteristiche simili, anche se più datate, del fratello maggiore ESX ma, almeno, è gratis. A proposito di gratis, tra i più famosi sistemi di virtualizzazione resi disponibili gratuitamente ci sono Microsoft Virtual PC e Virtual Server.

:: Microsoft? No, grazie

Le due proposte di casa Microsoft hanno cercato di inseguire il successo di VMWare senza, tuttavia, arrivare al suo livello di ottimizzazione.
In particolare, il controllo da parte dell'utente delle macchine virtuali è sempre risultato abbastanza scadente e non offre le caratteristiche di portabilità e gli snapshot tipici della maggior parte dei prodotti VMWare. A differenza di questi, però, l'ottimizzazione degli ambienti Windows on Windows, specialmente installando le Virtual Machine Additions, è risultata migliore. Purtroppo, sia Virtual Server che Virtual PC mancano di una caratteristica fondamentale che ha fatto il successo di VMWare: la possibilità di rendere visibile un disco fisico a una macchina virtuale.

:: Dischi e 3D? No!

Ogni sistema di virtualizzazione, infatti, ha debolezze comuni dovute a come funziona l'hardware sottostante.
Nel dettaglio dei dischi, l'accesso in lettura e scrittura avviene tramite una o più testine specifiche e studiate per l'uso da parte di un singolo computer. Quando ci sono più macchine virtuali in lettura e/o scrittura, l'accesso al disco viene regolato tramite semafori e il sistema rallenta. Per evitarlo, alcuni sistemi, come quelli proposti da VMWare, permettono di dedicare un disco fisico a una macchina virtuale, eliminando il problema.

Altri, come quelli proposti da Microsoft, non lo permettono, costringendo a ricorrere a condivisioni di rete. Altro problema comune della virtualizzazione è lo sfruttamento delle schede video. In genere vengono emulate schede video con caratteristiche di base e questo rende impossibile l'uso di sistemi di grafica o di videogiochi in ambienti virtualizzati. Per ora, gli unici sistemi che permettono in modo nativo lo sfruttamento degli hardware video sono stati creati per utenti Mac: VMWare Fusion 2, Parallels Desktop for Mac, QuickTransit e pochi altri. Per architettura x86 Xen propone un sistema, Xen-GL, usato anche da altri sistemi come VMWare Workstation, QEmu o KVM che non è uno standard degli ambienti non virtuali e, per questo, non dà garanzie di compatibilità. Altro grande punto debole riguarda le connessioni USB. Per loro caratteristiche tecniche, queste non sono virtualizzabili: in normali condizioni, un device USB non può essere usato contemporaneamente da più macchine virtuali.

Questo ha dato vita a una serie di soluzioni alternative usate da quasi tutti i produttori per consentire visibilità dell'USB anche alle macchine virtuali. Nell'elenco di chi supporta i dispositivi USB, però, sono assenti Virtual PC e Virtual Server: un problema di non poco conto vista l'importanza che i dispositivi USB stanno assumendo sempre più.



Si fa presto a mettere online un video con YouTube ma quali meccanismi stanno alla base di queste tecnologie?

FILMATI E STREAMING

Il sistema è semplice: ci si registra, si fa qualche clic, si sceglie un filmato sul computer e si dà l'OK. Dopo poco, il filmato è già disponibile su YouTube o su FaceBook o su decine di altre piattaforme. Poi ci si siede tranquilli e si fanno videochiamate agli amici per raccontare la novità. Due operazioni apparentemente senza collegamenti tecnici tra loro che, però, vedono come filo conduttore l'uso dei video. La differenza, tuttavia, è fondamentale: i video di YouTube sono statici, inseriti in un luogo preciso e sono rivedibili a piacere mentre le videochiamate sono trasmesse in tempo reale. Tecnicamente, la differenza è abissale e colloca le due operazioni in due contesti completamente diversi.

:: DVD o TV?

La collocazione di un video su un sito non ha alcuna differenza tecnica con l'inserimento di qualsiasi altro materiale: si tratta di un semplice file video che viene messo in download. Le videochiamate, invece, utilizzano in modo nativo una tecnica chiamata streaming: le immagini vengono catturate, codificate e inviate agli utenti collegati in tempo reale o con discrepanze temporali ridotte al minimo. È la stessa differenza che c'è tra i DVD e la televisione e, come avviene anche per questi media, le cose si possono mescolare, registrando un DVD dalla TV o mandando in onda in TV un film. In campo informatico, il rimescolamento avviene quando si decide di usare qualche tool e registrare le videochiamate, ottenendo file che possono essere visti e rivisti. Oppure quando si prendono file video, si codificano e si trasmettono agli utenti tramite streaming. Esattamente questa operazione è quella che viene fatta da YouTube: il filmato depositato sul suo server dall'utente viene codificato usando un sistema particolare e inviato al client Flash di chi lo ha richiesto. Questo invio permette all'utente di vedere il filmato fin da subito, senza



dover prelevare l'intero file dal server di YouTube. Addirittura, il procedimento di codifica dello streaming supera i problemi di compatibilità di formati video diversi, fornendo un flusso di informazioni standard e interpretabile da qualsiasi player di Adobe senza dover scaricare plugin aggiuntivi come avviene, invece, per i filmati contenuti in file. Per questo motivo è banale vedere filmati tramite YouTube o altre piattaforme di streaming mentre può diventare un'avventura vedere file video se non si hanno installati i CODEC corretti.

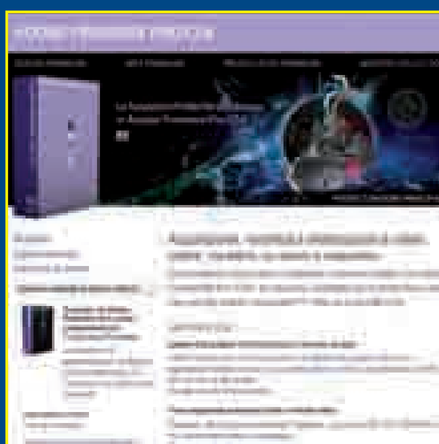
:: Guardare l'erba crescere

Da un punto di vista funzionale, tuttavia, i due sistemi di gestione video hanno vite completamente separate. Lo streaming, pur usato per inviare filmati statici agli utenti, è studiato per la visione di avvenimenti in tempo reale: immagini da webcam, videogiornali, riprese in diretta da telecamere e così via. I file video statici hanno, invece, lo scopo di conservare quello che lo streaming ha già mostrato e permetterne anche tutte le elaborazioni successive. Dal punto di vista tecnico, trattandosi di due sistemi funzionalmente tanto diversi, l'hardware e il software coinvolti hanno differenze abissali. Per la creazione di filmati in file basta un eventuale sistema di ripresa, come una webcam, un sistema di registrazione, un sistema di archiviazione. Questo è il motivo fondamentale per cui è oggi piuttosto semplice creare filmati casalinghi: quaslasi moderno computer con scheda di acquisizione video oppure con una economica webcam può trasformarsi in un registratore video. Salvo poi permettere anche il montaggio del girato, la sua codifica, l'editing in DVD e la masterizzazione. Il tutto con una spesa ridotta a un semplice computer.



Oggi si assiste spesso alla nascita di diverse web radio di discreto successo, sia grazie alla semplicità di questo tipo di streaming che alla nascita di piattaforme, come via streaming.com, che lo rendono facile per tutti.

Per lo streaming le cose cambiano moltissimo. Oltre all'attrezzatura di acquisizione video è necessario avere un'area di storage, in genere un computer con dischi molto veloci, in cui memorizzare in via transitoria il materiale girato. Poi serve un computer, con un processore veloce, per la codifica del video preso dalla storage. Poi serve un altro computer, dotato di connessioni veloci, capace di prelevare il lavoro di codifica fatto e inviarlo agli utenti che richiedono il filmato. Infine serve, naturalmente, una connessione col resto della rete capace di supportare l'invio dei dati. Teoricamente, un solo computer potrebbe fare tutto il lavoro ma il suo costo sarebbe elevatissimo a fronte di una qualità del servizio scadente. Per questo motivo, in genere, vengono usati più computer che si occupano di fare il vero streaming, magari collegati a molte linee dati, così da amplificare sia la banda disponibile per le trasmissioni che la capacità di soddisfare molti client contemporaneamente.



Adobe Premiere Pro è la soluzione di editing video professionale più usata e a costo più abbordabile. Chi non ha un migliaio di euro per crearsi, in parte, una regia video in tempo reale?



Le Web TV oggi disponibili, come quelle RAI, sono spesso ricodifiche delle Tv tradizionali e non hanno una personalità autonoma e indipendente, anche se il mercato potrebbe essere più appetibile per gli inserzionisti.

:: Una TV fatta in casa?

Le cose si complicano se si desidera avere anche un certo livello di qualità oltre che dare un servizio di streaming perché saranno necessari più sistemi di ripresa da usare in contemporanea, una regia in tempo reale capace di intervenire tra la codifica e lo streaming vero e proprio e anche un supporto da parte di file video normali per riempire le pause. Sarebbe necessario riprodurre, in pratica, tutte le attrezzature di uno studio televisivo tradizionale, con i conseguenti costi hardware e software. Proprio quest'ultimo punto, il software di elaborazione video, è una ulteriore nota dolente: diversamente dall'elaborazione audio, quella video costa moltissimo e richiede hardware più potente. Per questo motivo non solo non esistono televisioni fai da te via Internet mentre le radio casalinghe sono sempre più diffuse.



Quando si tratta di file video è importante disporre di archivi. Per fortuna, le storage attuali vanno da quelle casalinghe da 1 Tb che costano qualche centinaio di euro fino ad armadi storage dal costo di svariati migliaia di euro ma con uno spazio di svariate decine di Tb.

Lenny: il sistema operativo universale



L'attesa nuova distribuzione Debian, che si presenta con il nome in codice di Lenny supporta ben 12 architetture. La quantità di software rilasciato è tale da riempire fino a 5 DVD (o 32 cd), ma è possibile realizzare mini-installazioni o addirittura micro-installazioni per farla girare anche in ambienti embedded come iPhone.

:: Processo di installazione

Per la prima volta nella storia di Debian, viene rilasciato un installer grafico, ma la modalità testuale resta comunque la scelta di default (ciò che funziona davvero bene difficilmente viene messo da parte nell'open-source). In verità non c'è da aspettarsi molto: sostanzialmente consente di ripercorrere gli step del menu testuale in modo grafico e navigando con il mouse. Proseguendo vediamo che la sezione dedicata al partizionamento dell'hard-disk è rimasta spartana come in precedenza, così come il menu di installazione in generale e che la configurazione del boot loadar (grub) è un po' complessa: va indicato il UUID (device ID) del file-system nella nuova versione, invece del nome del device come in precedenza. Questo vuol dire che va ripristinata questa configurazione in caso di crash dell'hard-disk per consentire a grub di avviare il sistema. Come plus però, l'installer grafico di Debian 5.0 permette di configurare il RAID (mentre su Ubuntu si deve obbligatoriamente ricorrere all'installer testuale per questo).
Il riconoscimento dell'hardware è buono, ma dal momento che Debian adotta come politica il rilascio di solo software veramente gratuito e OpenSource, i file contenenti il firmware (proprietario) dei vari adattatori wifi, non sono presenti nei dischi di installazione e vanno scaricati dal repository etichettato come "non-free". Persino Firefox e Thunderbird sono presenti "senza marchio" rispettivamente con i nomi di Iceweasel e Icedove.
Il problema di questo approccio si pone su quei computer dove il collegamento avviene tramite una scheda wifi perché si dovranno scaricare tali pacchetti altrove oppure su recenti chipset che potrebbero richiedere un upgrade manuale a una versione non del tutto stabile del kernel di Linux.



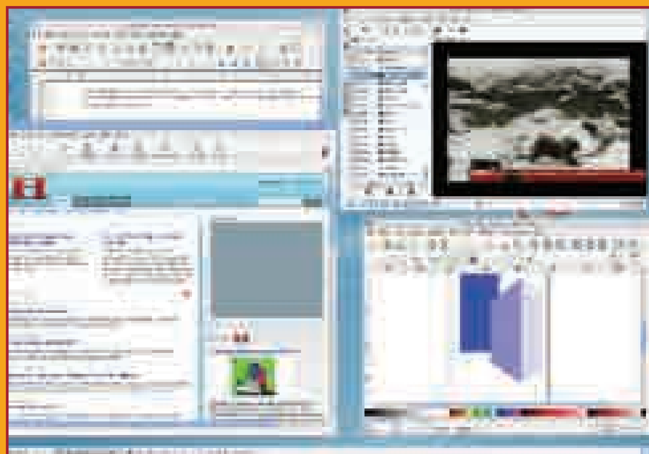
Questa è la schermata in cui effettuare il partizionamento dell'hard-disk.

Dopo circa due anni di lavoro il team di sviluppo di Debian ha finalmente rilasciato la nuova versione 5.0 della famosa distribuzione open-source di Linux

:: Principali novità

L'aspetto sicurezza è sempre la priorità del progetto Debian. Con Lenny quindi, sono stati integrati nella versione di default le ultime patch di OpenSSH e i pacchetti di SELinux (il rafforzamento di sicurezza di Linux) che precedentemente venivano solo consigliati. Sono state riviste le pacchettizzazioni del kernel che permettono di gestire le ultime versioni del kernel di Linux dove cambiano diverse caratteristiche (in particolare c'è l'introduzione di OpenVZ, una modalità di virtualizzazione del kernel); inoltre sono state unificate tra i diversi processori riconducibili alla famiglia 686 (AMD/Intel/VIA) semplificando sia la manutenzione che l'installazione.

A differenza dei predecessori, Lenny è davvero una distribuzione Java-friendly, che include di default OpenJDK della Sun, il compilatore Java e l'interprete Java bytecode. Inoltre è stato introdotto X.org 7.3, il motore grafico che in questa versione non richiede più alcuna pre-configurazione dell'hardware e carica di default driver Open-Source per l'hardware riconosciuto. Ovviamente è sempre possibile, in una fase successiva, installare driver commerciali, ove rilasciati (es. Nvidia), ma non è presente un aggiornamento automatizzato nonostante compaiano nel repository non-free.



Ecco l'attesa nuova versione di Debian all'opera. Niente di particolare,le novità sono tutte "sotto il cofano".

:: Come si presenta Lenny

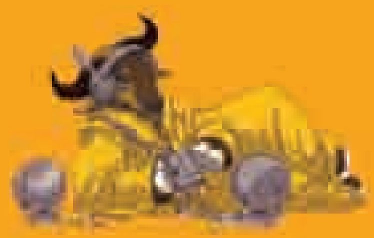
L'ambiente grafico di base è Gnome, così come nella distribuzione Ubuntu 8.10, non a caso derivata dalla Debian. Questo fatto fa sì che le due distribuzioni si somiglino davvero molto, anche nella struttura dei menu, ma la Debian non provvede a installare di default, ad esempio l'infrastruttura di gestione di Bluetooth, e utilizza in generale delle versioni software più vecchie rispetto a Ubuntu (ma Ubuntu adotta come politica quella di uscire ogni 6 mesi con una distro derivata dalla Debian e con i pacchetti aggiornati), perché fa sempre parte della sua filosofia quella di rilasciare solo le versioni collaudate e giudicate veramente più stabili e affidabili a discapito di essere sempre pronti all'ultima novità. Questa scelta si riflette anche con il kernel che viene rilasciato, solitamente, molto più datato rispetto all'ultima release disponibile.

Tutto questo non elimina la possibilità di personalizzare completamente la distribuzione e aggiornare automaticamente (ad esempio da repository testing) i pacchetti alle ultime versioni rilasciate o aggiungere a mano, o da fonti non ufficiali, pacchetti non ancora inseriti (in passato si faceva così ad esempio per testare i diversi JDK non ufficialmente inseriti).

Dal punto di vista del multimediale, Lenny si posiziona davvero bene, ma solo dopo aver attivato i repository non-free. Totem e Kaffeine, insieme ai vari codec pre-installati permettono di mandare in play tutti i formati audio e video più diffusi, ma è possibile anche utilizzare periferiche DVB-T (digitale terrestre). Tramite il filesystem UDF 2.5 è poi possibile avere anche il supporto per Blu-Ray.



Primo avvio, Lenny ci dà il benvenuto: ecco la finestra di Login.



:: Usabilità

Lenny si presenta come una distribuzione davvero stabile e un po' più user-friendly della precedente (la 4.0, Etch). La configurazione di rete ad esempio, grazie a Network Manager, è davvero semplice ed è possibile impostare diversi profili per chi si collega da più luoghi (casa, ufficio, ...) e deve gestire diverse configurazioni. Inoltre il set-up di stampanti che si collegano via usb è stato automatizzato come su Ubuntu. Sono presenti diversi software di virtualizzazione (Xen, Qemu e VirtualBox) e diversi pacchetti sono stati ricompilati utilizzando le ottimizzazioni offerte dal compilatore GCC, volte ad aumentare la sicurezza. Questo dovrebbe rendere diversi pacchetti fondamentali più resistenti agli attacchi, in particolare se si parla di MySQL, PostgreSQL e Nagios. Grazie a Lenny, ora possono utilizzare la Debian sia utenti esperti che novizi, soprattutto per le migliorie introdotte sulla configurazione dei collegamenti di rete, gestione delle stampanti. Può essere scomodo dover scaricare separatamente i firmware delle schede di rete, ma è un piccolo prezzo da pagare per una distribuzione famosa per l'attenzione alla sicurezza e stabilità e manifesto dell'open-source. In generale l'installazione non è proprio semplice, ma fa parte del gioco capire realmente cosa stiamo facendo quando ci viene richiesto quale boot-loader scegliere e quale "profilo" vogliamo dare al sistema che stiamo installando: la Debian è la distribuzione più vicina allo spirito open-source a disposizione!



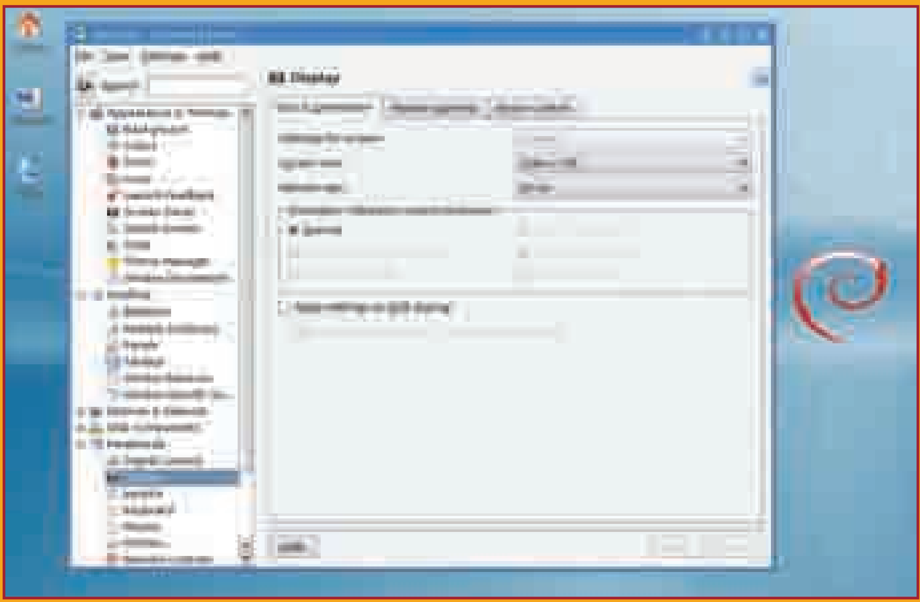
Se vi appare questo popup non preoccupatevi. È tutto sotto controllo e il sistema si installerà ugualmente.

:: Debian 5.0 Live

Per chi avesse qualche dubbio a testare una vera installazione Debian può provare una distribuzione live acui viene data grande importanza. Con quella ufficiale vengono infatti rilasciate svariate versioni live (scaricabili dal sito **http://debian-live.alioth.debian.org**).

Noi abbiamo provato la versione x86 32-bit con Gnome, scaricando la iso e lanciandola in una macchina virtuale. Il boot è chiaramente un po' lento: il sistema in versione live deve gestire il caricamento e la decompressione del sistema operativo e delle applicazioni basandosi unicamente sulla ram (simulata nel nostro caso), ma permette di poter valutare l'effetto che avrebbe quella configurazione a nostra disposizione prima di metter mano all'hard-disk (che sia vero o virtuale l'effetto non cambia).

Dobbiamo dire che Virtual PC di Microsoft non è in grado di farla girare (la versione 2007 andava direttamente in crash al boot). Con una versione vmware non troppo recente, il kernel di Lenny incontra qualche difficoltà (che viene segnalata in un pop-up nel desktop), ma il sistema si avvia correttamente è ci ritroviamo una versione di Linux gradevole e già pronta con gli ormai insostituibili Firefox e OpenOffice, per citare due dei software preinstallati.
La macchina virtuale effettuava il NAT verso l'host connesso a Internet ed è stato possibile fin da subito navigare senza dover configurare nulla: il server DHCP è già attivo e ci ha messi online. E navigando nei menu troviamo diverse applicazioni pronte all'uso che danno la sensazione di avere tra le mani più Ubuntu che una storica Debian.



IL Pannello di controllo di Lenny è facile anche per i neofiti del pinguino.

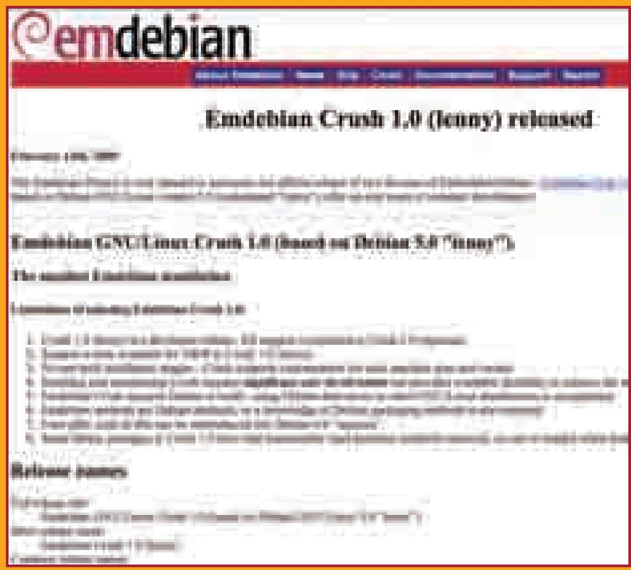
:: Embedian 1.0

Tra le novità introdotte da Lenny c'è anche il rilascio ufficiale di Embedian 1.0, l'ambiente di sviluppo open-source che permette di cross-compilare la Debian per architetture embedded (ad esempio basate su processori ARM utilizzati anche in diversi telefonini). Il vantaggio principale di Embedian rispetto a Debian è la dimensione, in secondo luogo la minor richiesta di risorse.

:: Cosa viene fornito con Embedian

Embedian 1.0 raggruppa il toolchain, ossia l'insieme degli strumenti di compilazione e debug specifici per le piattaforme embedded (arm, powerpc, 68000, mips, ...) supportate da Linux, ma soprattutto dei pacchetti specifici realizzati per piattaforme povere di risorse:

- **Embedian Crush:** una mini-distribuzione di Debian basata su Busybox che include un ambiente grafico GTK+2, disponibile solo per piattaforma ARM. L'installazione richiede una pesante interazione da parte dell'utente dal momento che non sono disponibili immagini pre-compilate e ogni installazione va personalizzata per la specifica piattaforma embedded;
- **Root Filesystem for ARM:** un'immagine di root che ha solo busy box senza "essentials" come perl;
- **Embedian Grip:** un'installazione intermedia che permette di utilizzare anche i pacchetti di Lenny; infatti l'installazione tipica è quella di partire con il setup di Lenny, installare solo il base system e attraverso dei pacchetti di migrazione (pre-seeding) installare Grip e tutti quelli che si desidera inserire fintanto che c'è spazio nella memoria di massa del dispositivo;
- **Cross building tools:** vengono continuamente mantenuti i pacchetti di sviluppo del Toolchain e la generazione del root filesystem.



All'indirizzo www.embedian.org possiamo scaricare l'ultima versione oltre a tutta la documentazione ufficiale disponibile.

:: Lo stato di Embedian

Embedian è presentato come work-in-progress. La scelta di rilasciarlo come versione 1.0 insieme a Lenny rappresenta sicuramente un passo importante, ma il lavoro è tuttora in corso e soggetto a miglioramenti. L'interesse per Linux nei dispositivi embedded è cresciuto enormemente negli ultimi anni e la scommessa del progetto Debian è quella di realizzare una piattaforma davvero open-source e gratuita anche in questo campo.

Massimiliano Brasile

LENNY & IPHONE



Lo scorso novembre il kernel di linux 2.6 è stato portato anche sulla piattaforma di iPhone, supportando sia la prima che la seconda generazione del telefonino (vedi **www.iphone-dev.org/planetbeing/LINUX-README.txt**). Mancava il supporto per diversi driver e il porting era abbastanza grezzo, ma nei fatti stava girando un altro sistema operativo su un dispositivo commerciale venduto come scatola chiusa! Nel kernel erano state inseriti il driver Framebuffer per la visualizzazione grafica, il driver seriale, la gestione della USB, la gestione di Interrupt, MMU, clock, ecc. ed era in porting openiboot per il boot automatico di linux che doveva aggiungere un po' tutto il resto (supporto in lettura/scrittura per la NAND, supporto Wireless, touchscreen, gestione audio, accelerometro, supporto di telefonia in banda base). Poi grazie a Embedian è stato possibile effettuare il porting di Debian su iPhone (vedi **http://linuxoniphone.blogspot.com/2008/12/debian-on-iphone-linux.html**) che compare quindi tra le piattaforme supportate.

Finalmente in edicola la prima rivista
PER SCARICARE ULTRAVELOCE
TUTTO quello che vuoi



Chiedila subito al tuo edicolante!